Darkode
Analyse de la structure relationnelle d’un réseau de hackers d’élite

Benoît Dupont

Chaire de recherche du Canada en Cybersécurité

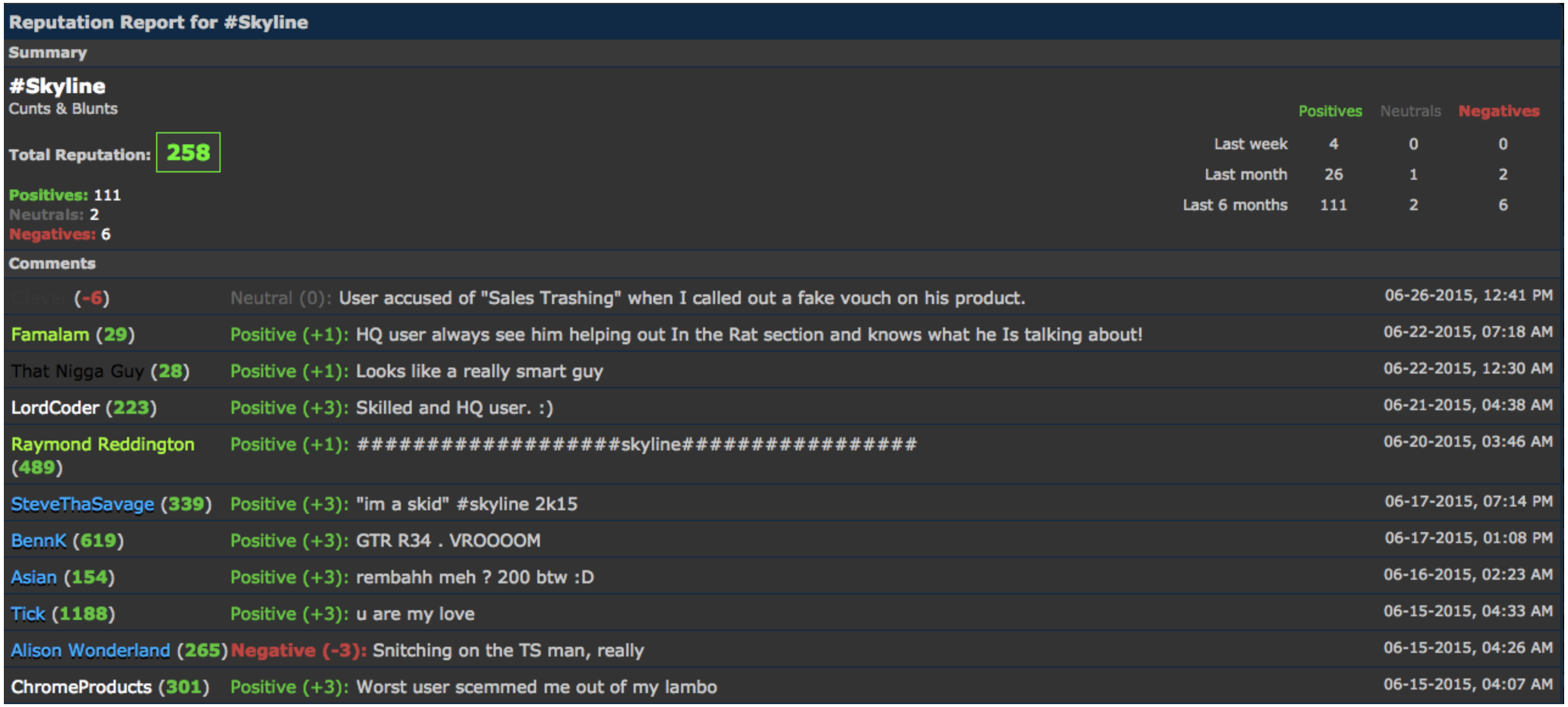
École de criminologie

Université de Montréal

Myth of the lone hacker

The online offender dilemma

Large scale reputation systems…



Reputation Report for #Skyline

Summary

#Skyline
Cunts & Blunts

Total Reputation: 258

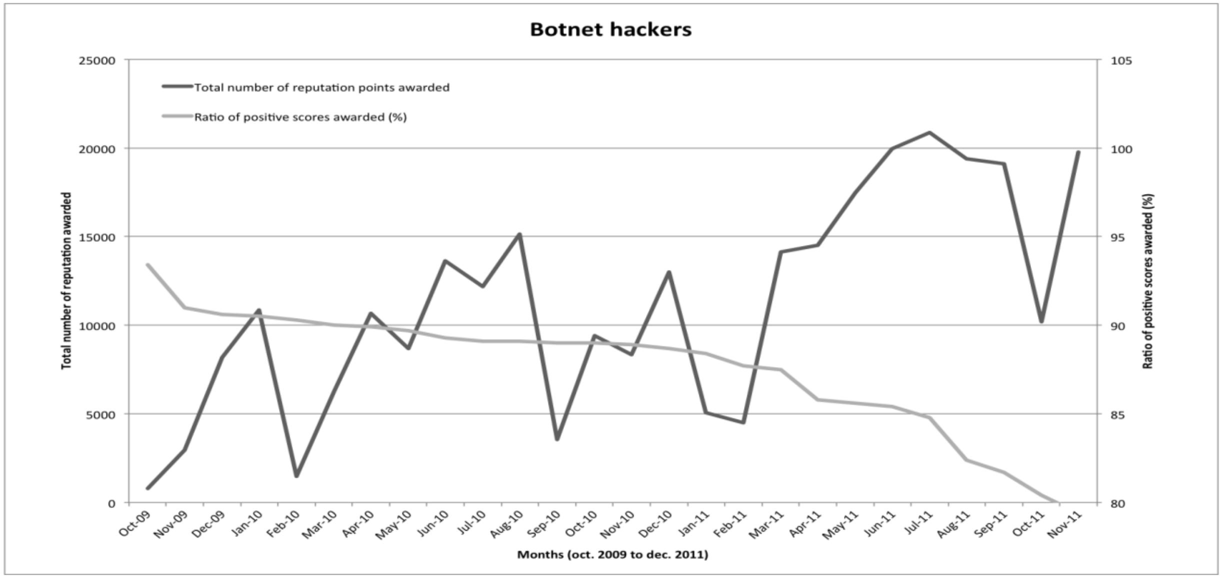
Positives: 111
Neutrals: 2
Negatives: 6

	Positives	Neutrals	Negatives
Last week	4	0	0
Last month	26	1	2
Last 6 months	111	2	6

Comments

Clayer (-6)	Neutral (0): User accused of "Sales Trashing" when I called out a fake vouch on his product.	06-26-2015, 12:41 PM
Famalam (29)	Positive (+1): HQ user always see him helping out In the Rat section and knows what he Is talking about!	06-22-2015, 07:18 AM
That Nigga Guy (28)	Positive (+1): Looks like a really smart guy	06-22-2015, 12:30 AM
LordCoder (223)	Positive (+3): Skilled and HQ user. :)	06-21-2015, 04:38 AM
Raymond Reddington (489)	Positive (+1): #################skyline################	06-20-2015, 03:46 AM
SteveThaSavage (339)	Positive (+3): "im a skid" #skyline 2k15	06-17-2015, 07:14 PM
BennK (619)	Positive (+3): GTR R34 . VROOOOM	06-17-2015, 01:08 PM
Asian (154)	Positive (+3): rembahh meh ? 200 btw :D	06-16-2015, 02:23 AM
Tick (1188)	Positive (+3): u are my love	06-15-2015, 04:33 AM
Alison Wonderland (265)	Negative (-3): Snitching on the TS man, really	06-15-2015, 04:26 AM
ChromeProducts (301)	Positive (+3): Worst user scemmed me out of my lambo	06-15-2015, 04:07 AM

… are not very reliable



R (-0.73**). P<0,01**

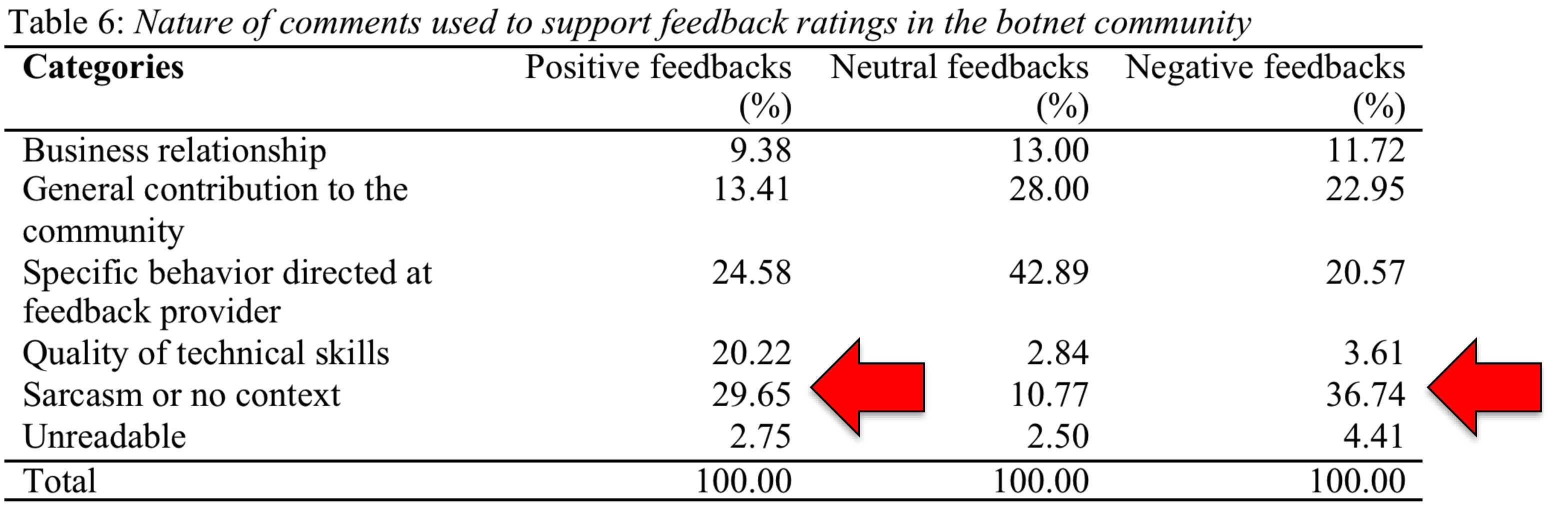


Table 6: *Nature of comments used to support feedback ratings in the botnet community*

Categories	Positive feedbacks (%)	Neutral feedbacks (%)	Negative feedbacks (%)
Business relationship	9.38	13.00	11.72
General contribution to the community	13.41	28.00	22.95
Specific behavior directed at feedback provider	24.58	42.89	20.57
Quality of technical skills	20.22	2.84	3.61
Sarcasm or no context	29.65	10.77	36.74
Unreadable	2.75	2.50	4.41
Total	100.00	100.00	100.00

The private club model

- "The most dangerous cybercrime forum in the world" according to the FBI
- Open: 2007- 2015
- Purpose: elite underground marketplace for high quality products and services (e.g. exploit kits, botnets, software, coding services, databases, 0day exploits, etc.)
- Approximately 450-500 English speaking members from around the world

Creation: 2007

Matjaz Skorjanc
27-year old Slovenian hacker
Aka: Iserdo
Butterfly/Mariposa botnet
Arrested in 2010
Sentenced to 58-month jail term (Dec. 2013)

Daniel Placek
27-year old US hacker
Aka: Nocen, Loki, Juggernaut
Credential harvesting software & botnets
Arrested in 2010
cooperated for 5 years with investigation
Pleaded guilty (sentence sought: 6-12 months)
Now a network engineer at Swick Technologies

Administration

2010

Johan Anders Gudmunds takes over as admin
27-year old Swedish hacker
Aka: Mafi, Crim, Synthet!c
Author of the exploit kit CrimePack, and operator of a 50,000 nodes botnet (Blazebot)
Arrested in 2015

Administration

2013: After a massive infiltration of a large number of law enforcement agents and security researchers in the forum, Mafi “resigns” as administrator

Duties taken over by: **Sp3cial1st**

Unlike previous admins, the main contribution of Sp3cial1st isn’t his technical skills, but a will to massively expand the membership while being very selective in order to prevent suspicious members from being admitted (see next slide)

Arrest: still at large

Darkode’s structure

- Three tiered system

  Level 0: *FreshFish* (introduction section, zero access)

  Level 1: *Trusted members* (access to the market-buys and sales)

  Level 2: *Highly trusted members* (administrators and influential members)

- invitation only forum
- Multi-step membership process

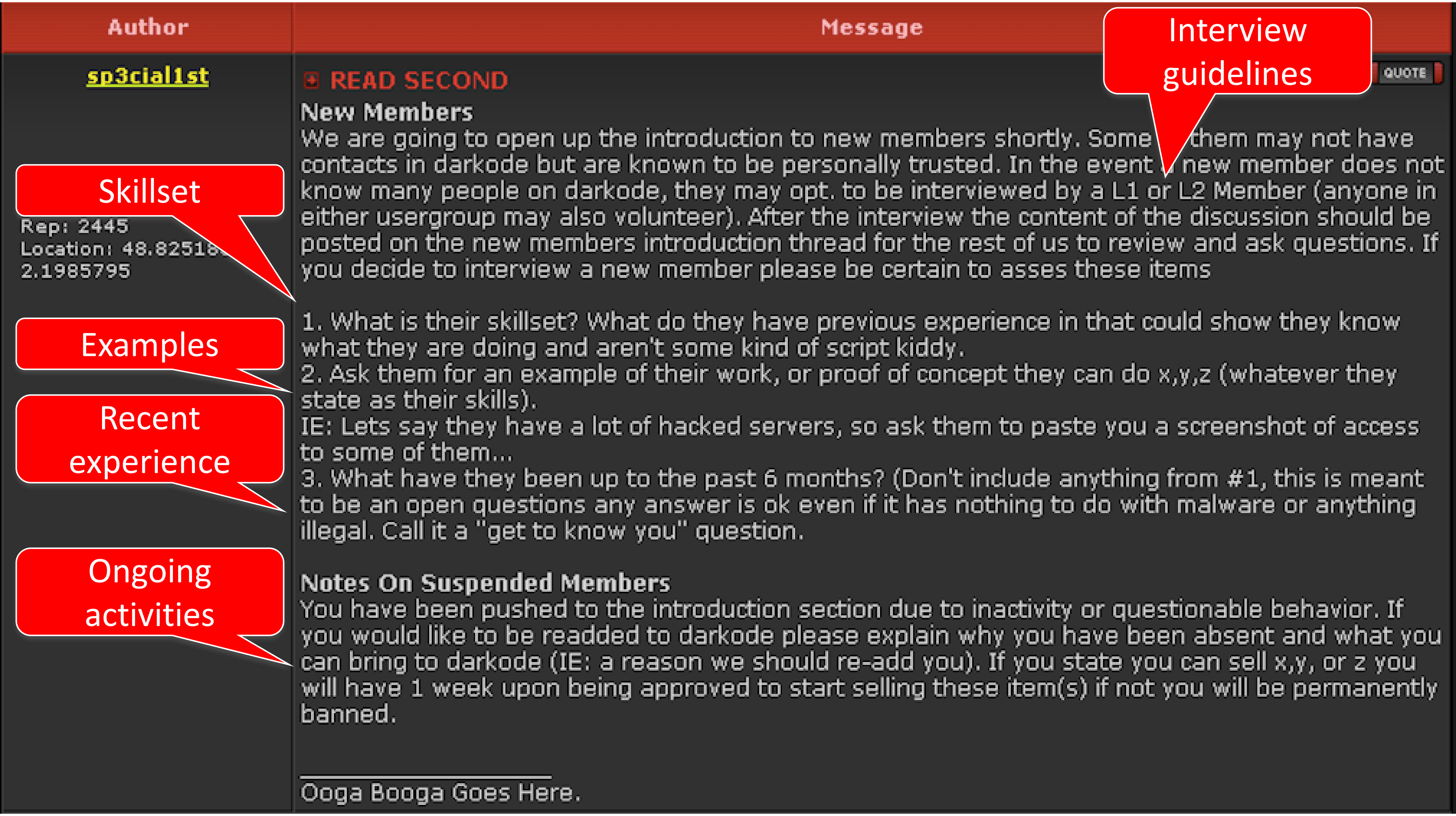
  1) Invitation by an existing member

  2) Introduction message to present skills/experience

  3) Interview with Level 2 or Level 1 member

  4) Public vote by the community

Admission process under Sp3cial1st



sp3cial1st

Rep: 2445
Location: 48.82518
2.1985795

READ SECOND

New Members

We are going to open up the introduction to new members shortly. Some them may not have contacts in darkode but are known to be personally trusted. In the event new member does not know many people on darkode, they may opt. to be interviewed by a L1 or L2 Member (anyone in either usergroup may also volunteer). After the interview the content of the discussion should be posted on the new members introduction thread for the rest of us to review and ask questions. If you decide to interview a new member please be certain to asses these items

1. What is their skillset? What do they have previous experience in that could show they know what they are doing and aren't some kind of script kiddy.
2. Ask them for an example of their work, or proof of concept they can do x,y,z (whatever they state as their skills).
IE: Lets say they have a lot of hacked servers, so ask them to paste you a screenshot of access to some of them...
3. What have they been up to the past 6 months? (Don't include anything from #1, this is meant to be an open questions any answer is ok even if it has nothing to do with malware or anything illegal. Call it a "get to know you" question.

Notes On Suspended Members

You have been pushed to the introduction section due to inactivity or questionable behavior. If you would like to be readded to darkode please explain why you have been absent and what you can bring to darkode (IE: a reason we should re-add you). If you state you can sell x,y, or z you will have 1 week upon being approved to start selling these item(s) if not you will be permanently banned.

Ooga Booga Goes Here.

Interview guidelines

Skillset

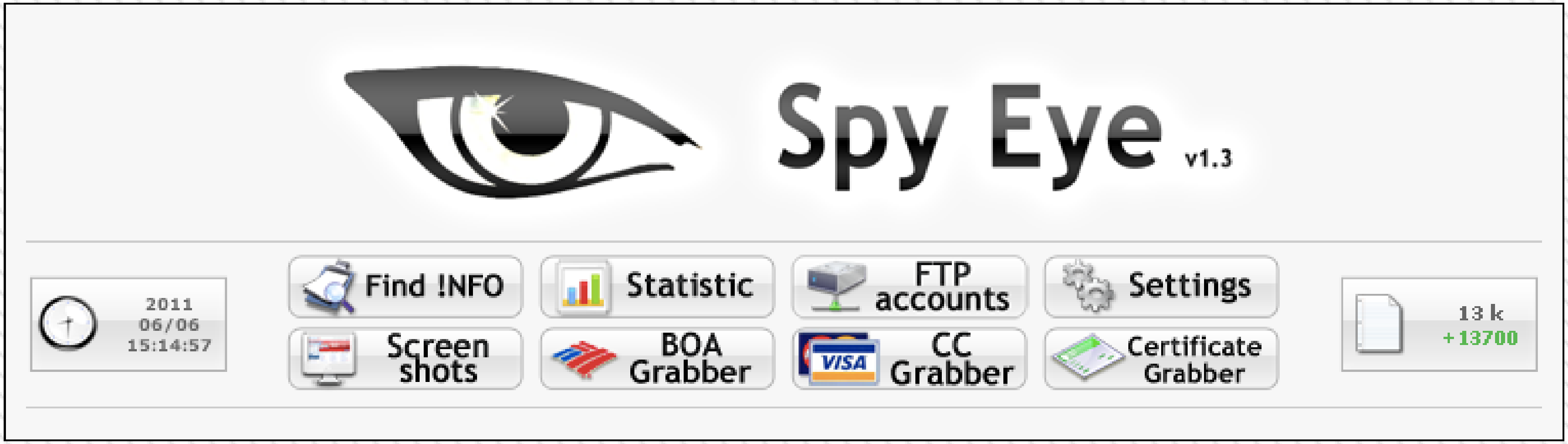
Examples

Recent experience

Ongoing activities

Darkode high-profile members

- *TinKode*: NASA hack [arrested Jan. 2012]
- *Alexudakov*: Phoenix exploit kit [arrested July 2012]
- *Bx1*: ZeuS botnet [arrested May 2013]
- *Gribodemon*: SpyEye [arrested Summer 2013]
- *Paunch*: Blackhole exploit kit [arrested Oct. 2013]
- *Phastman*: Facebook Spreader [arrested Summer 2015]
- Members from Lizard Squad forum [Sony Playstation DDoS attacks]



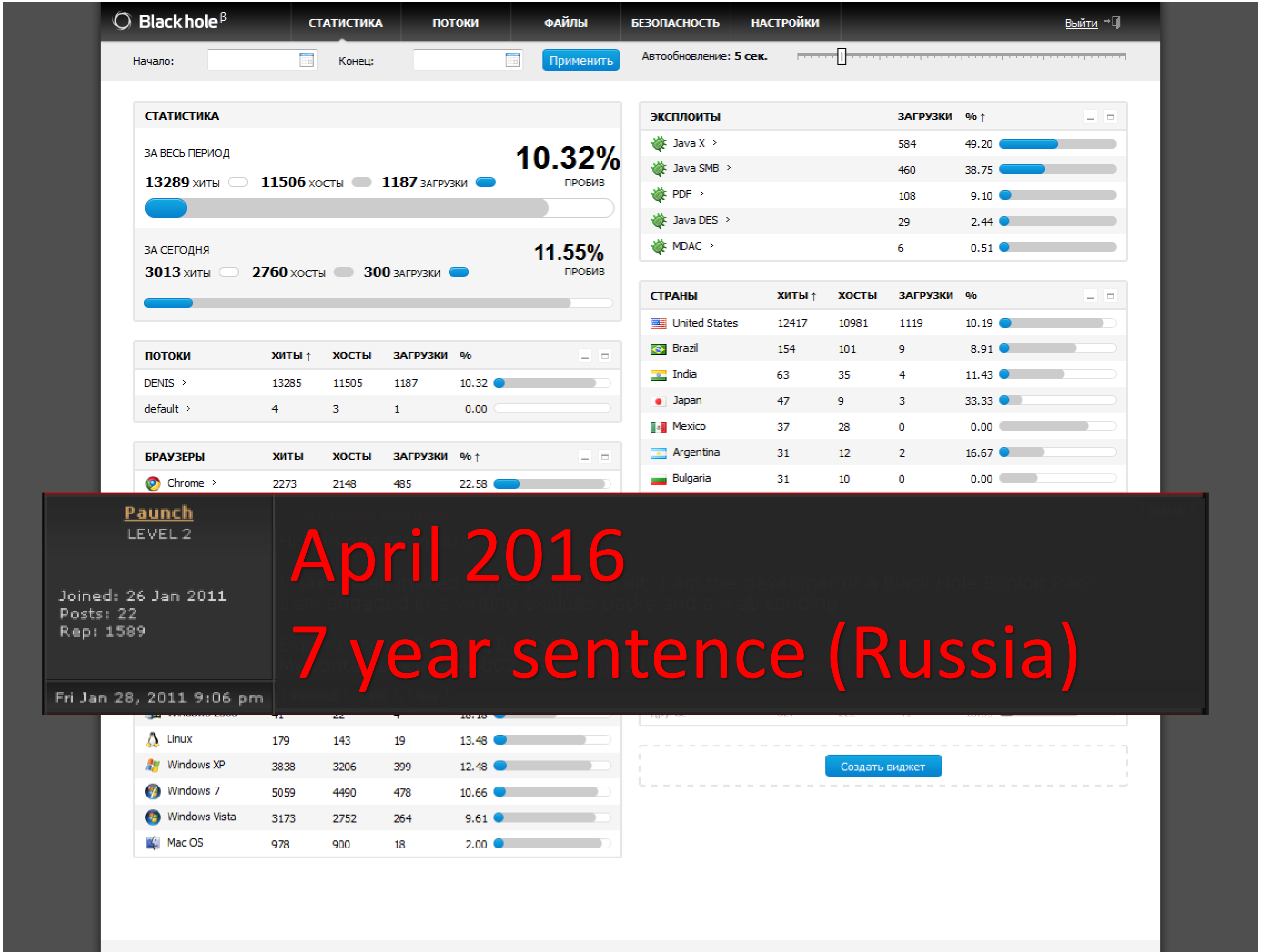
Selling Spreader BIN's (Facebook , USB , IM ....)

and many other methods and adding more in future (OFC by request) ....

April 2016

15 year sentence

(USA)



Начало: Конец: Автообновление: **5 сек.**

СТАТИСТИКА

ЗА ВЕСЬ ПЕРИОД

13289 ХИТЫ **11506** ХОСТЫ **1187** ЗАГРУЗКИ

10.32% ПРОБИВ

ЗА СЕГОДНЯ

3013 ХИТЫ **2760** ХОСТЫ **300** ЗАГРУЗКИ

11.55% ПРОБИВ

ПОТОКИ	ХИТЫ ↑	ХОСТЫ	ЗАГРУЗКИ	%
DENIS ›	13285	11505	1187	10.32
default ›	4	3	1	0.00

БРАУЗЕРЫ	ХИТЫ	ХОСТЫ	ЗАГРУЗКИ	% ↑
Chrome ›	2273	2148	485	22.58

Windows 2000	41	22	4	18.18
Linux	179	143	19	13.48
Windows XP	3838	3206	399	12.48
Windows 7	5059	4490	478	10.66
Windows Vista	3173	2752	264	9.61
Mac OS	978	900	18	2.00

ЭКСПЛОИТЫ	ЗАГРУЗКИ	% ↑
Java X ›	584	49.20
Java SMB ›	460	38.75
PDF ›	108	9.10
Java DES ›	29	2.44
MDAC ›	6	0.51

СТРАНЫ	ХИТЫ ↑	ХОСТЫ	ЗАГРУЗКИ	%
United States	12417	10981	1119	10.19
Brazil	154	101	9	8.91
India	63	35	4	11.43
Japan	47	9	3	33.33
Mexico	37	28	0	0.00
Argentina	31	12	2	16.67
Bulgaria	31	10	0	0.00

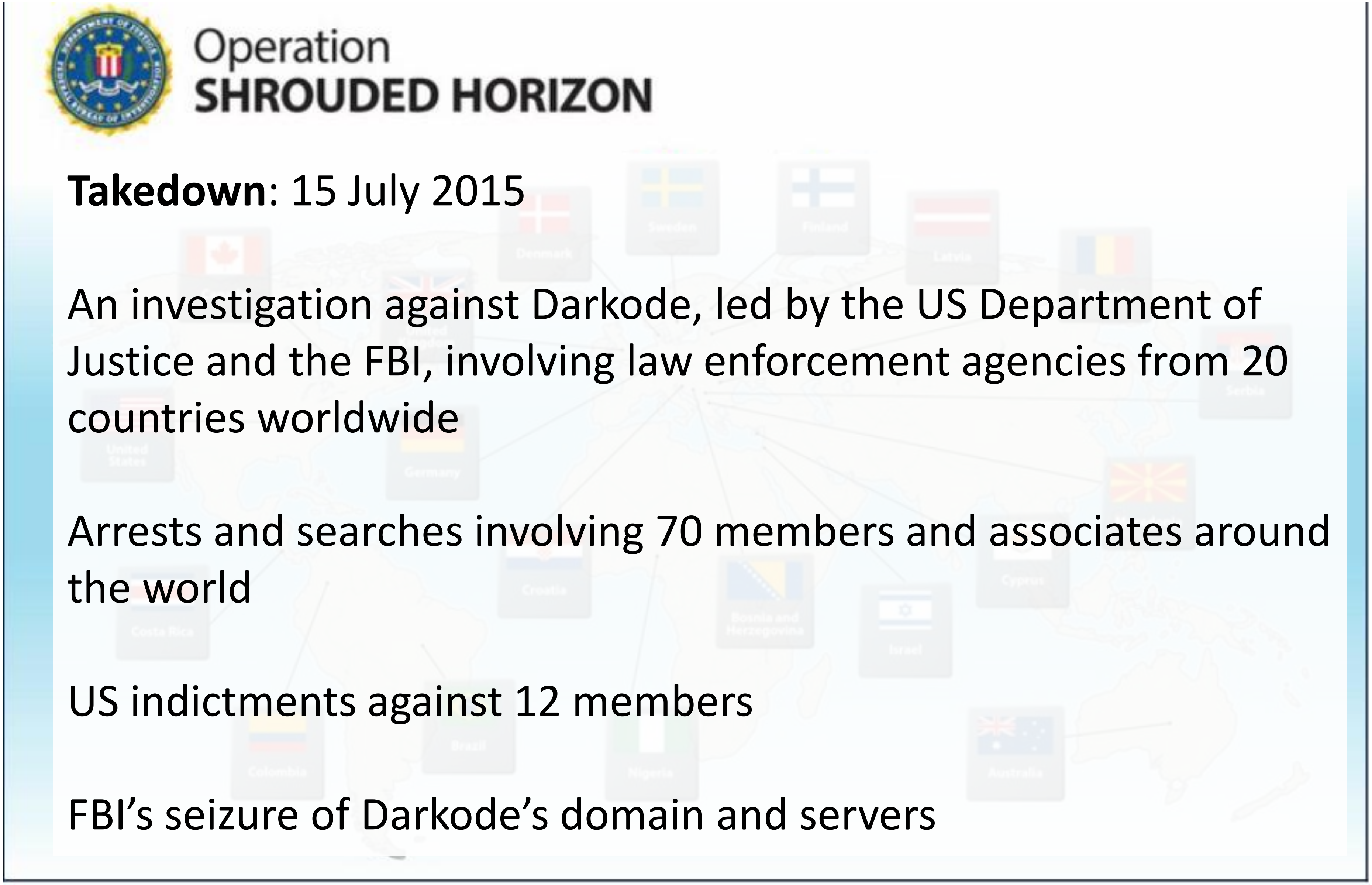
Paunch
LEVEL 2

Joined: 26 Jan 2011
Posts: 22
Rep: 1589

Fri Jan 28, 2011 9:06 pm

April 2016

7 year sentence (Russia)



Operation SHROUDED HORIZON

Takedown: 15 July 2015

An investigation against Darkode, led by the US Department of Justice and the FBI, involving law enforcement agencies from 20 countries worldwide

Arrests and searches involving 70 members and associates around the world

US indictments against 12 members

FBI’s seizure of Darkode’s domain and servers

The Darkode database

- ≈ 5000 screenshots (jpeg) from the Darkode forum
- Hacked by Xylitol [released April 1st, 2013]
- Posts cover 2009 - 2013

Data found in the DB:

- Membership list and links to the member’s level
- Products for sale
- Transaction reports (new products and buys)
- Tutorials
- Questions about specific problems
- Programming tips
- Malware analysis
- Name of hackers and of specific malware tools
- Hall of shame & conflict management procedures

Specific objectives

1) To understand the mechanisms underlying the admission of new members to the forum

What key information needs to be provided in intro message to be accepted in the forum?

2) To understand the forum’s structure using network analysis techniques

Pre- and post-arrest metrics

3) To understand the impact of Darkode on the malware scene (both products and services)

Qualitative analysis of marketing strategies and related business activities

Objective 1: Growth patterns of an elite hacking community

- 476 screenshots from the “introduction section”
- 344 applications analyzed (2009-2013)
- Qualitative analysis of the discussion following each application
- Coding of introductions based on the key information provided

  1: *Sponsors known inside the forum*

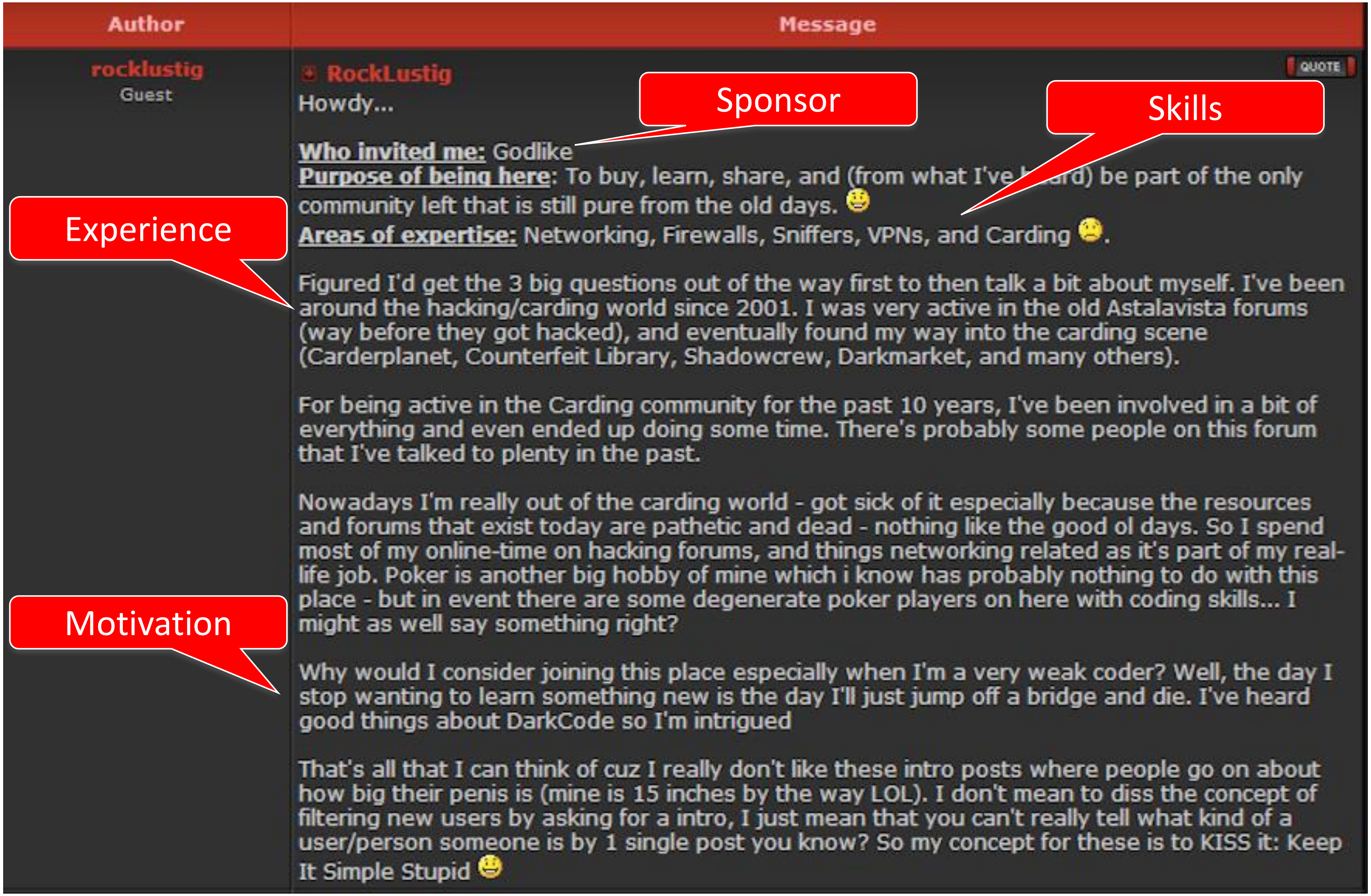
  2: *Experience in other forums*

  3: *Technical skills*

  4: *Business interests*

  5: *Products offered*

Example of an introduction message [RockLustig]



Sponsor

Skills

Experience

Motivation

rocklustig
Guest

RockLustig

Howdy...

Who invited me: Godlike
Purpose of being here: To buy, learn, share, and (from what I've heard) be part of the only community left that is still pure from the old days. 😃
Areas of expertise: Networking, Firewalls, Sniffers, VPNs, and Carding 🙁.

Figured I'd get the 3 big questions out of the way first to then talk a bit about myself. I've been around the hacking/carding world since 2001. I was very active in the old Astalavista forums (way before they got hacked), and eventually found my way into the carding scene (Carderplanet, Counterfeit Library, Shadowcrew, Darkmarket, and many others).

For being active in the Carding community for the past 10 years, I've been involved in a bit of everything and even ended up doing some time. There's probably some people on this forum that I've talked to plenty in the past.

Nowadays I'm really out of the carding world - got sick of it especially because the resources and forums that exist today are pathetic and dead - nothing like the good ol days. So I spend most of my online-time on hacking forums, and things networking related as it's part of my real-life job. Poker is another big hobby of mine which i know has probably nothing to do with this place - but in event there are some degenerate poker players on here with coding skills... I might as well say something right?

Why would I consider joining this place especially when I'm a very weak coder? Well, the day I stop wanting to learn something new is the day I'll just jump off a bridge and die. I've heard good things about DarkCode so I'm intrigued

That's all that I can think of cuz I really don't like these intro posts where people go on about how big their penis is (mine is 15 inches by the way LOL). I don't mean to diss the concept of filtering new users by asking for a intro, I just mean that you can't really tell what kind of a user/person someone is by 1 single post you know? So my concept for these is to KISS it: Keep It Simple Stupid 😃

Results’ overview

Approval rate: 94.5%

In their introduction message, *FreshFish* (new members without access to the forum) put forward 5 types of key information to elicit trust from existing members.

Here’s the proportion of those key information in the introduction messages.

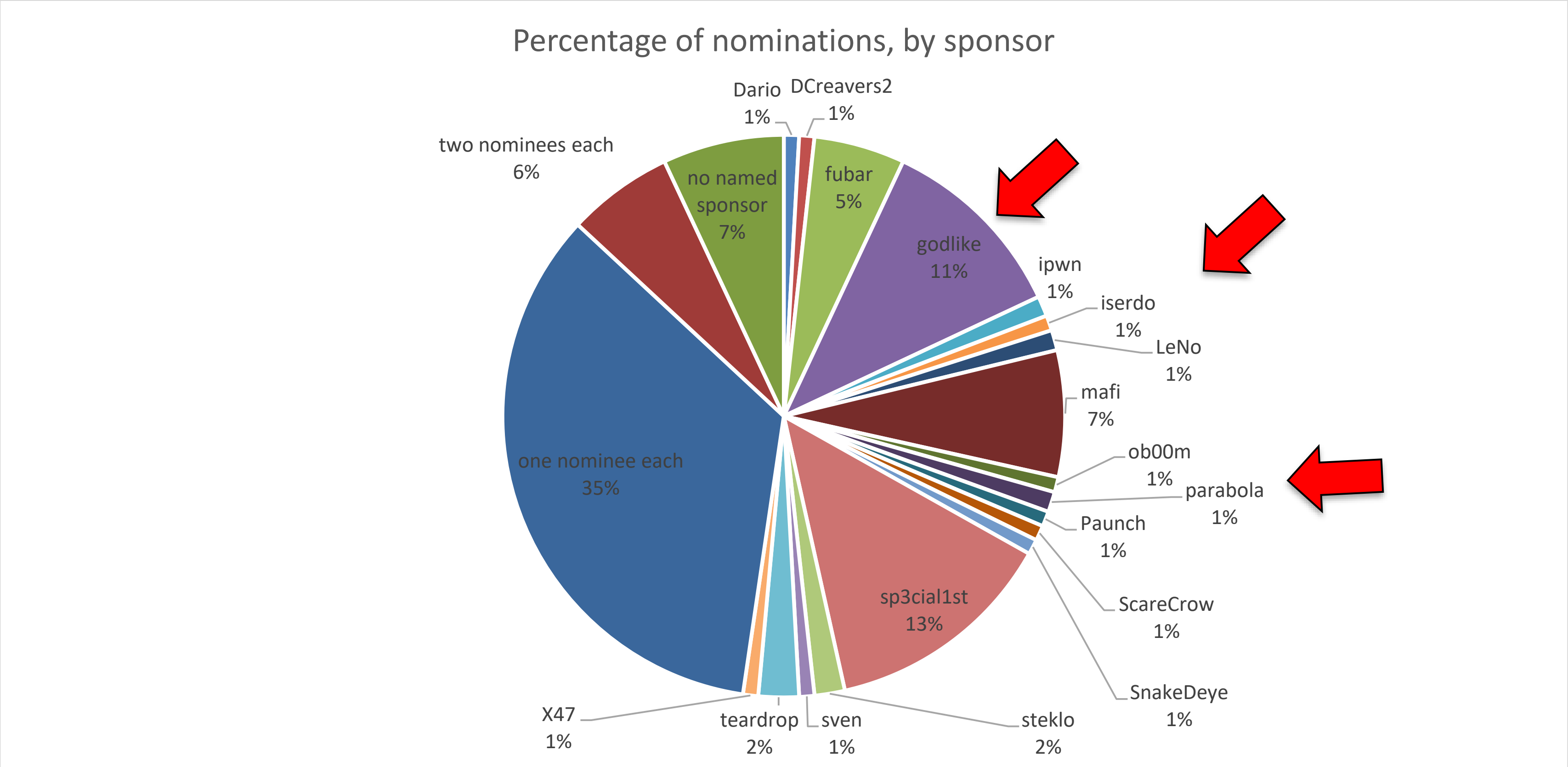
Introduction « *FreshFish* »

Categories	**Percentage**
Sponsor	83%
Experience	62%
Technical skills	67%
Business interests	54%
Products	55%

Sponsors

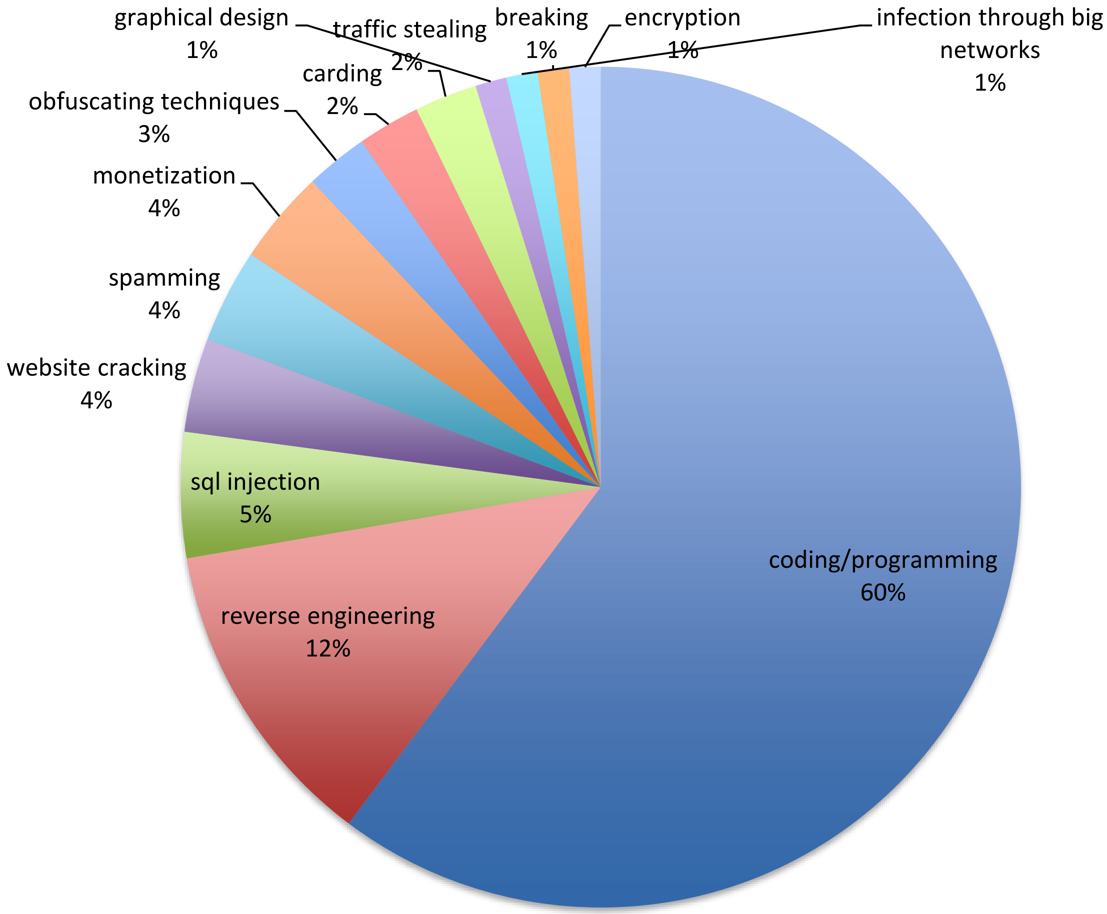
The 344 introductions acknowledge invitations (or nominations) extended by 119 Darkode members (average of 2.7 and median of 1 invitation converted per referrer, range: 1-46)

The four most influential recruiters (Sp3cial1st, G0dlike, Mafi, and Fubar) account for 36% of invitations



Technical skills

Distribution of technical skills that applicants claim and tools they can design/operate

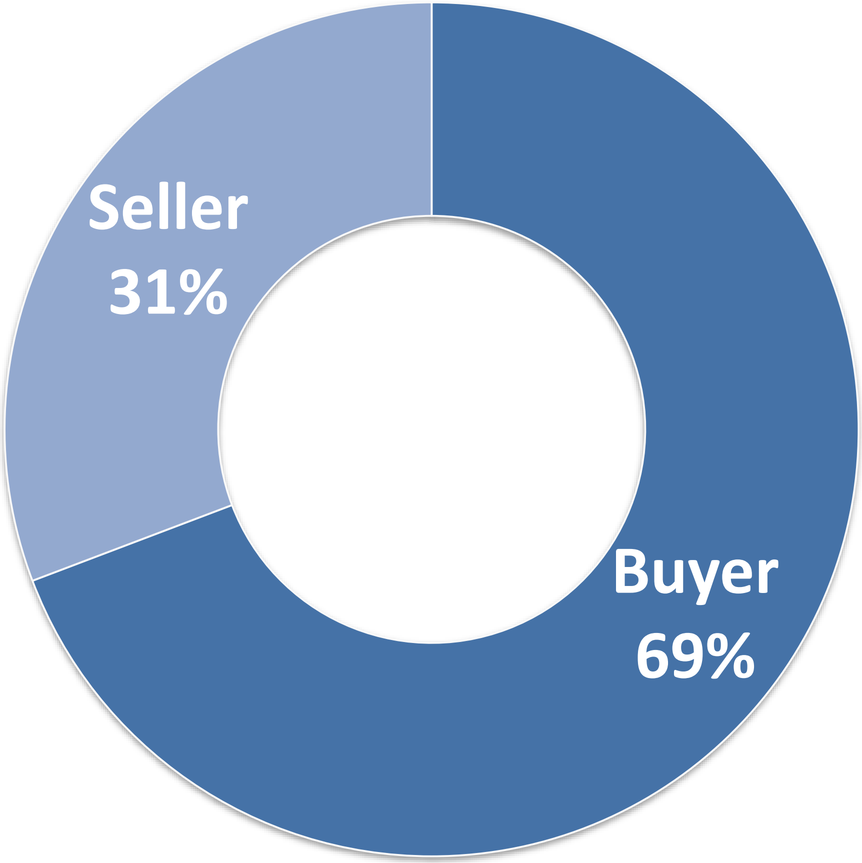


Specific tools and programs mentioned

Python, vb6, linux, xss, sqli, C/C++, html, ASM, Javascript, Nimrod, Vala, D, shells, databases, Windows, Linux, Php, Perl, Botnets, Exploit kits, Hacking proxys, ATMs…

Darkode: a seller’s market

The proportion of interest in buying and selling

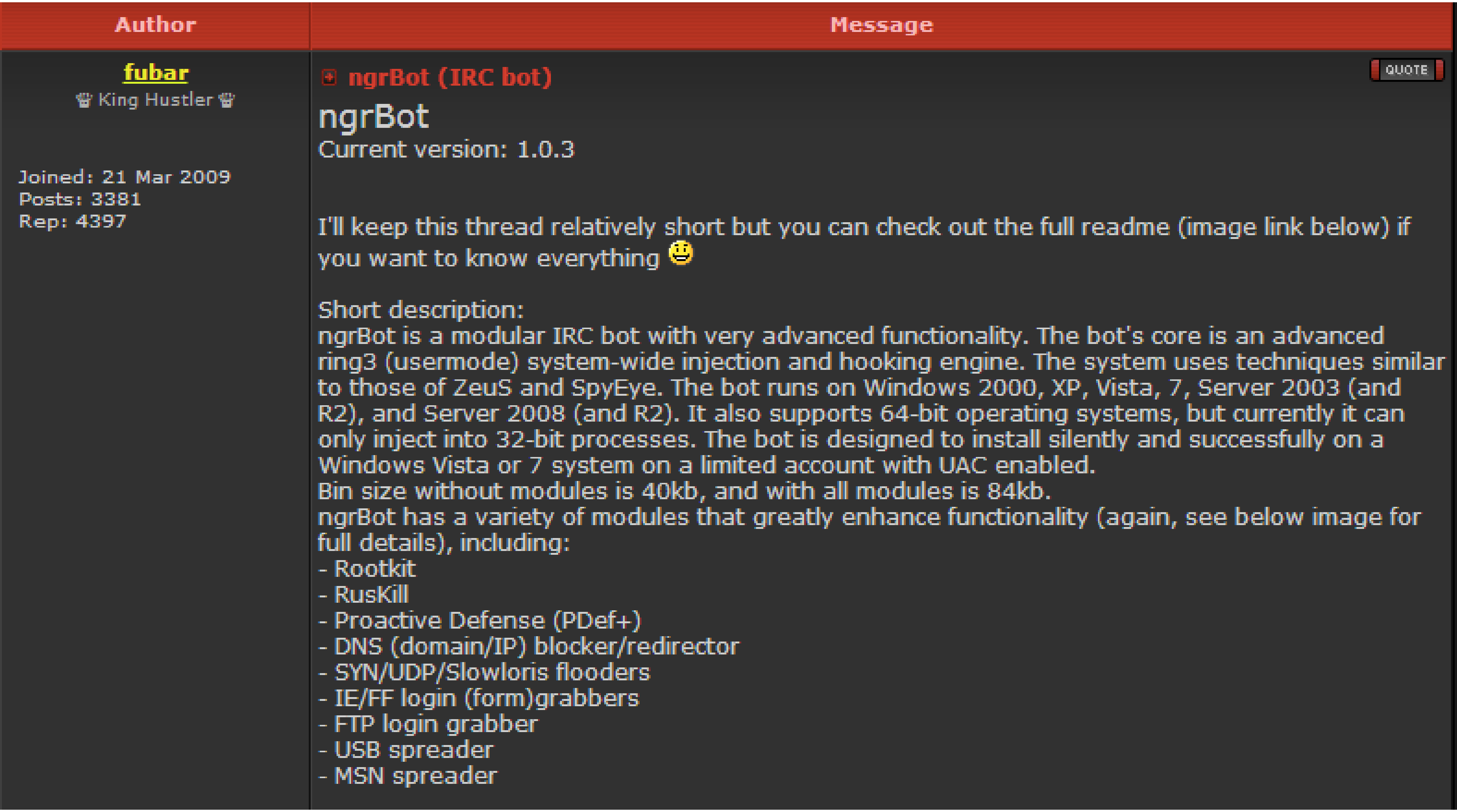


What is on demand:

- Rootkits
- Botnets
- Malware tools
- Codes
- C++ projects
- Exploits
- Database
- 0day
- Crypters
- Mails or accounts
- Trojans
- Proxies
- Traffic
- Software

Products

Also sold by established members and administrators themselves.



fubar

♛ King Hustler ♛

Joined: 21 Mar 2009
Posts: 3381
Rep: 4397

ngrBot (IRC bot)

ngrBot

Current version: 1.0.3

I'll keep this thread relatively short but you can check out the full readme (image link below) if you want to know everything 😃

Short description:
ngrBot is a modular IRC bot with very advanced functionality. The bot's core is an advanced ring3 (usermode) system-wide injection and hooking engine. The system uses techniques similar to those of ZeuS and SpyEye. The bot runs on Windows 2000, XP, Vista, 7, Server 2003 (and R2), and Server 2008 (and R2). It also supports 64-bit operating systems, but currently it can only inject into 32-bit processes. The bot is designed to install silently and successfully on a Windows Vista or 7 system on a limited account with UAC enabled.
Bin size without modules is 40kb, and with all modules is 84kb.
ngrBot has a variety of modules that greatly enhance functionality (again, see below image for full details), including:

- Rootkit
- RusKill
- Proactive Defense (PDef+)
- DNS (domain/IP) blocker/redirector
- SYN/UDP/Slowloris flooders
- IE/FF login (form)grabbers
- FTP login grabber
- USB spreader
- MSN spreader

Products

Sample of products and services advertised on Darkode.

Product Types		Product Names
Crypting tools	Ddos	Zeus
Coding shells	Exploitkits	Spyeye
Software	Rootkits	Citadel
Porn	Traffic (mails)	Yoshi
VPN	Bitcoin	Farenheit
BP (server, domain)	Databases	Eleonore
Installs accounts	Malware	AlHost
0day exploits	Phone numbers	Winlocker source code
Botnets	Accounts (Facebook, Hotmail, Yahoo, Paypal, academic)	Propack exploikit
Proxies		
Trojan		
Adverts systems		

Introductions’ outcomes

Each introduction is commented/vetted by existing members. Some offer welcome, others ask questions on specific skill or experience, or discuss the potential value added by the prospective member. DK members conclude their comments by a vote in favour or against the applicant’s admission. The table to the right lists the distribution of (mostly positive) comments across the five features presented above.

	Introductions	**Answers from existing members**
Categories mentioned	Percentage	Percentage
Sponsor	83%	16%
Experience	62%	56%
Technical skills	67%	20%
Business	54%	34%
Products	55%	--%

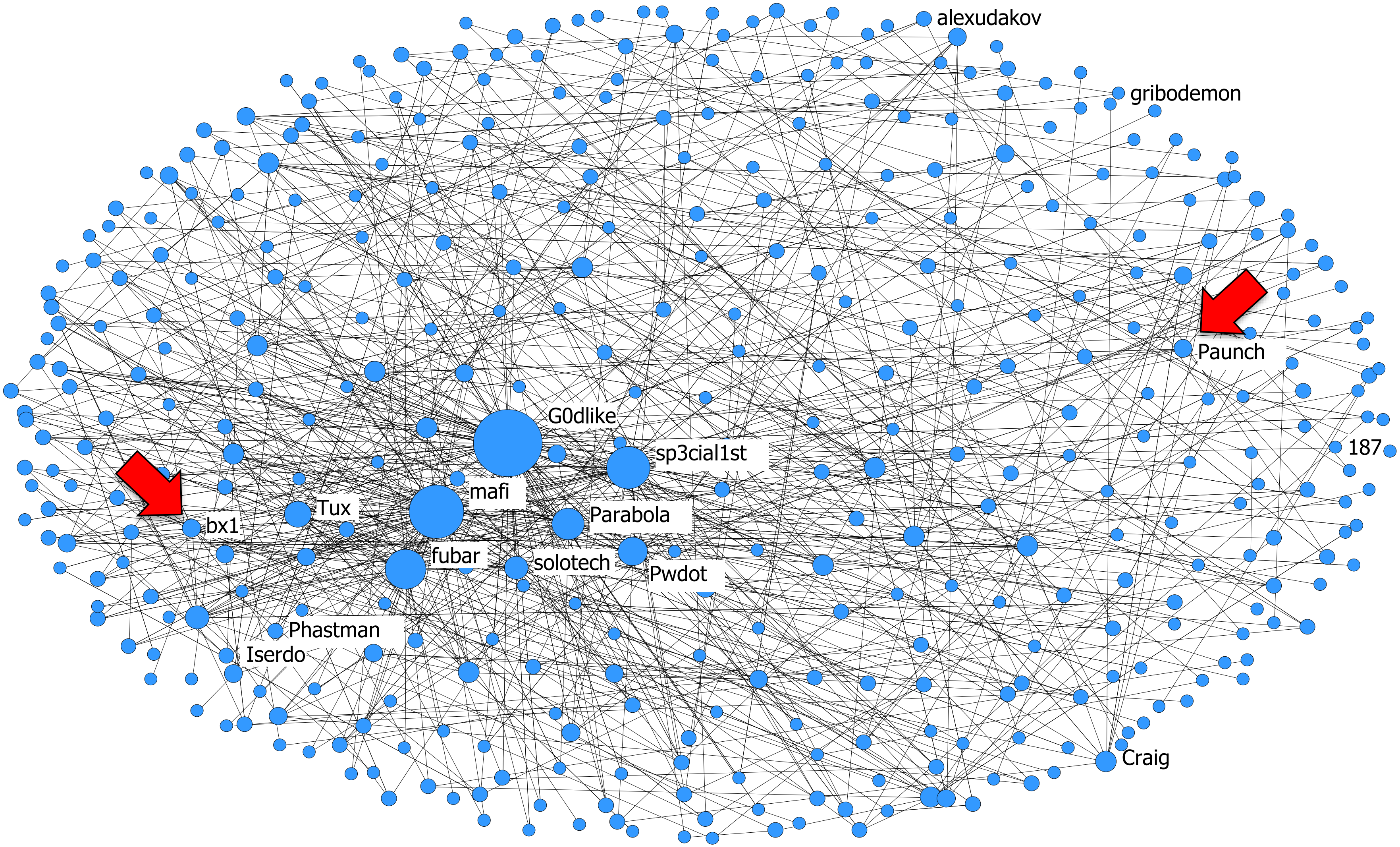
Objective 2: Map the network structure of this forum

Data:

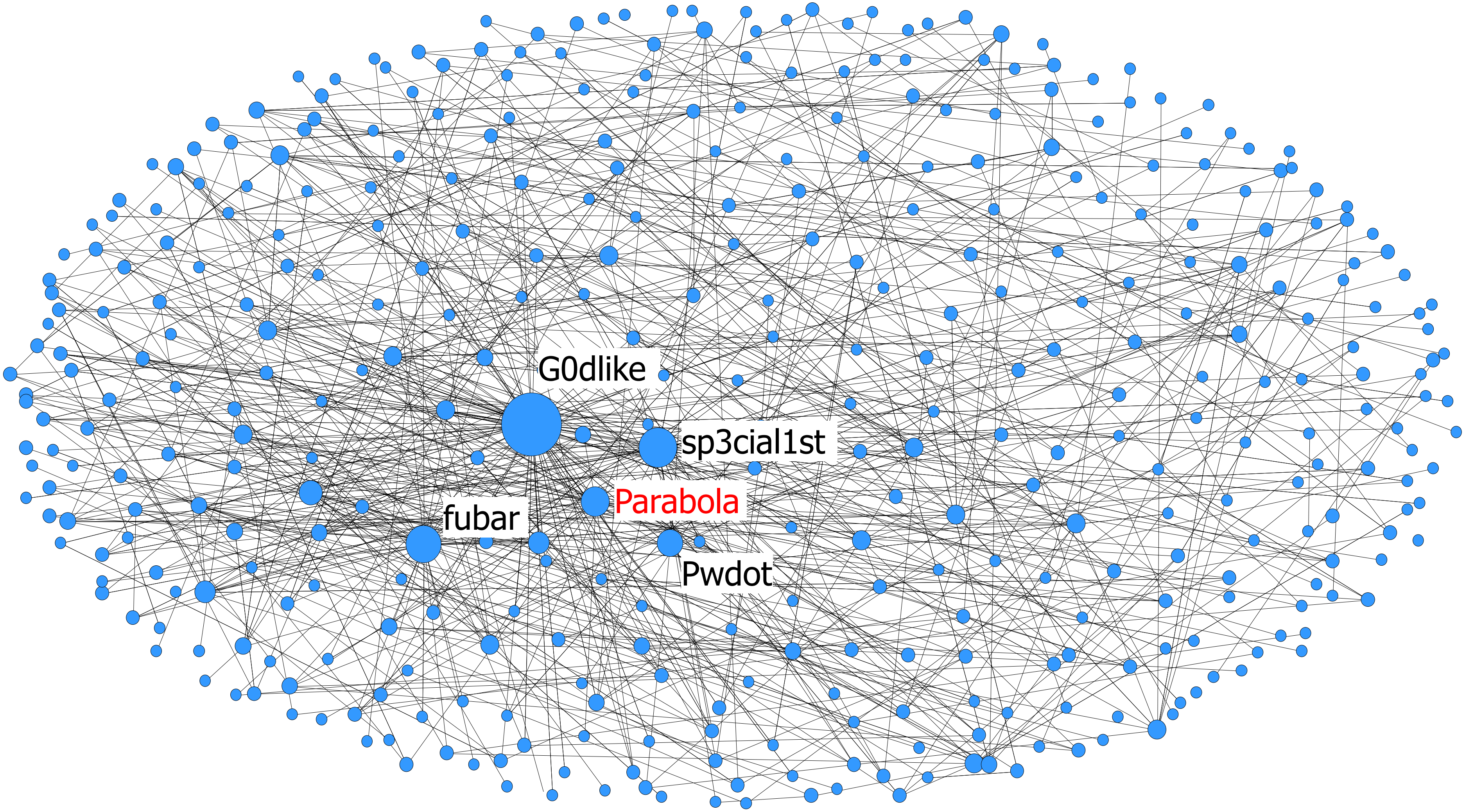
- 476 screenshots from the “introduction section”
- 404 members (2009-2013)
- Qualitative analysis and coding of introductions and comments
- Posts contain information describing social ties between members: *FreshFish* names sponsor; sponsor confirms he knows the applicant; other members state prior collaborations and ties that are meant as a vetting mechanism; etc.

Pre-arrest network

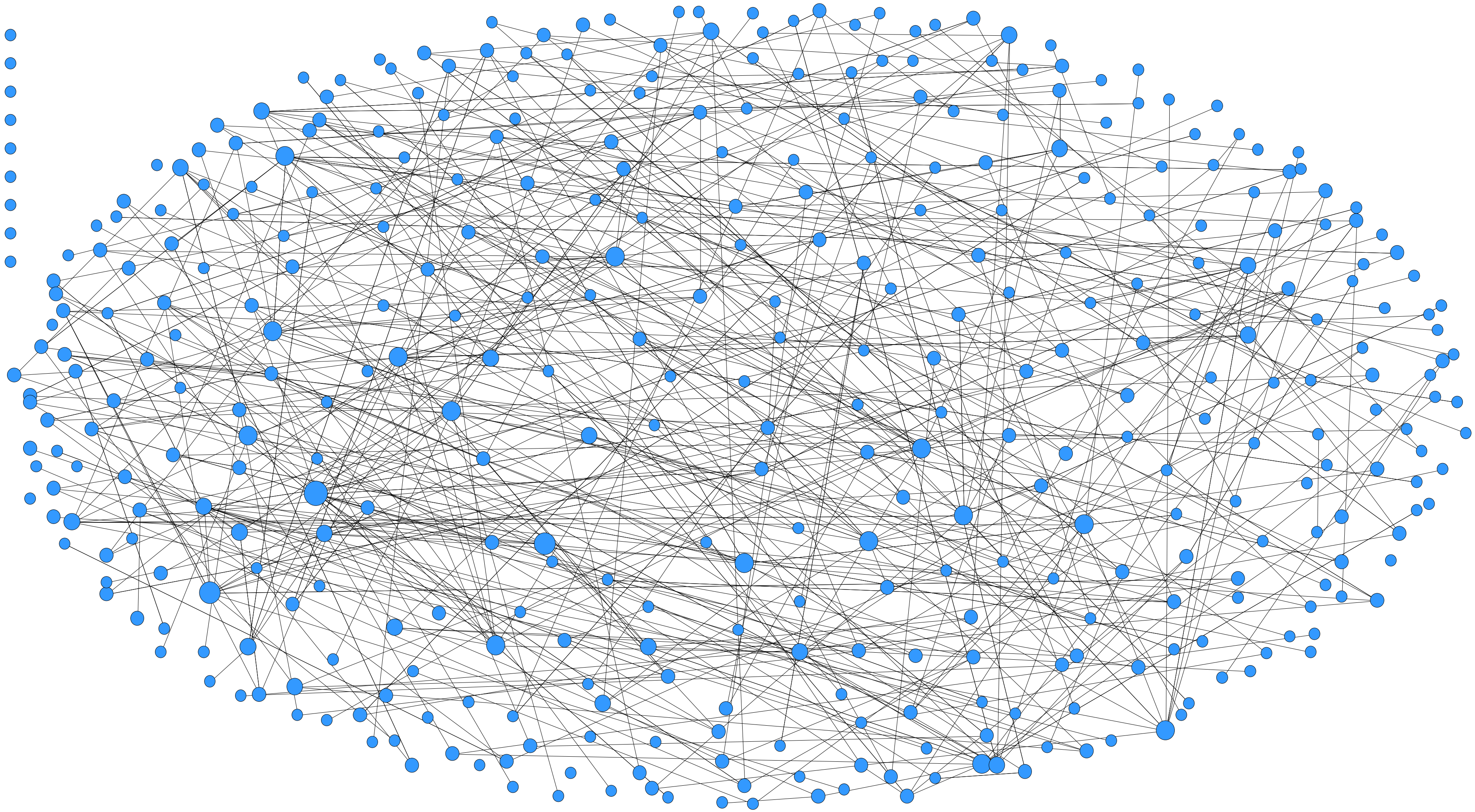
404 nodes – Density: 0.006 – average degree: 2.6 [1-69]



Post-arrest network (extrapolated)



Optimal arrest outcomes

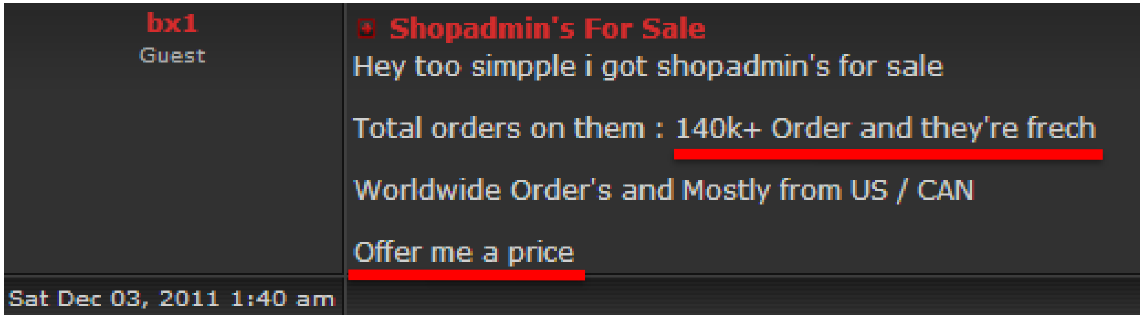


Objective 3: To understand the marketing strategies and nature of business activities on the malware scene (both products and services)

Data:

- 811 threads from the “marketplace” and “hall of shame fame” sections
- Qualitative analysis and coding of products, services, prices and negotiations
- Ongoing analysis

The tough business life of the hacker



bx1
Guest

Shopadmin's For Sale

Hey too simpple i got shopadmin's for sale

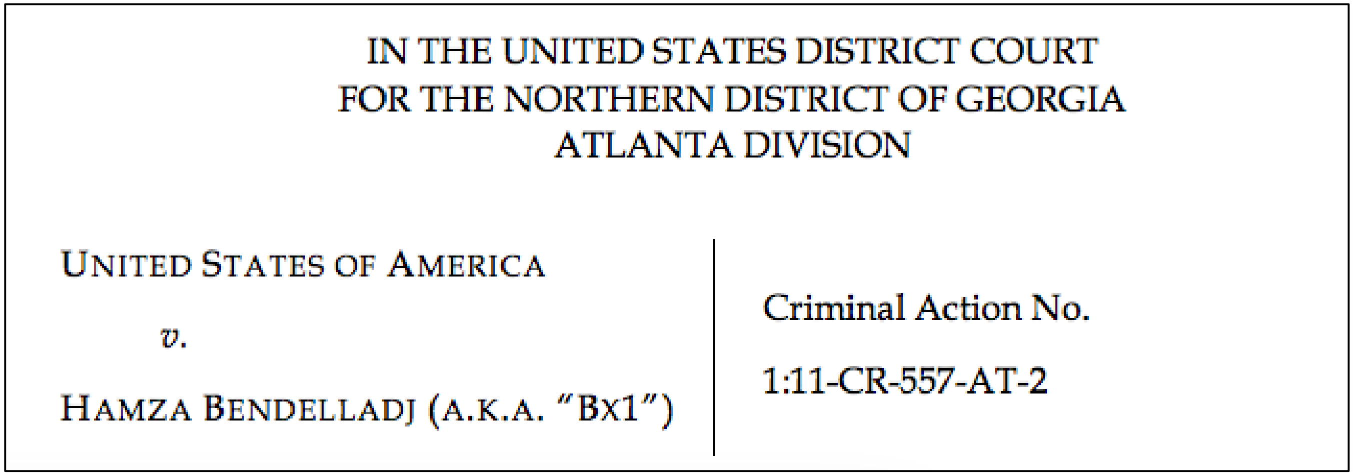
Total orders on them : 140k+ Order and they're frech

Worldwide Order's and Mostly from US / CAN

Offer me a price

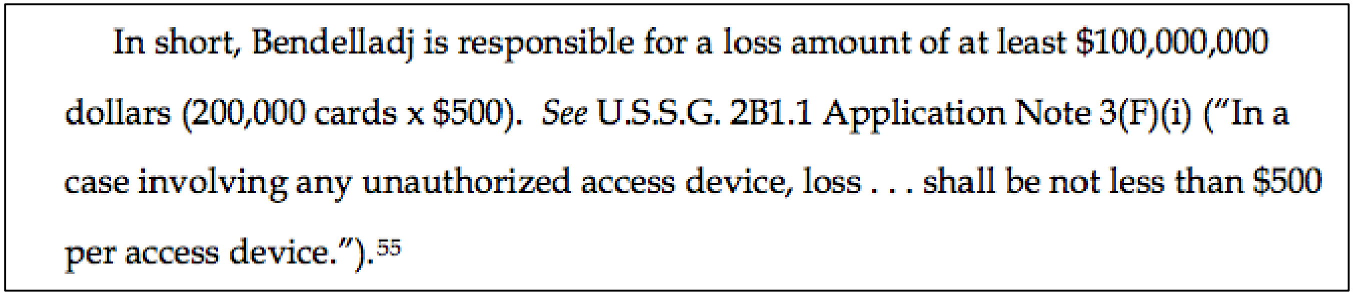
Sat Dec 03, 2011 1:40 am

$70,000,000



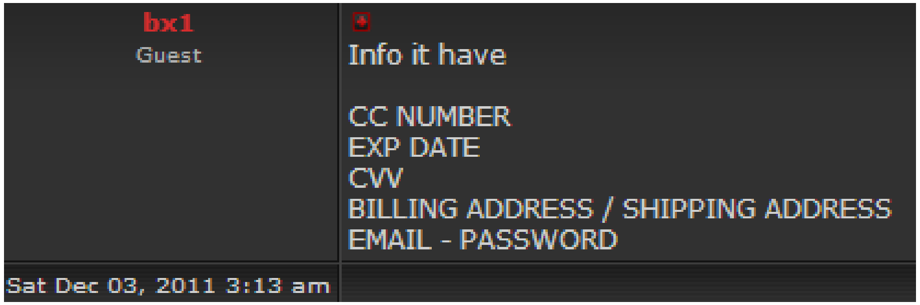
IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

UNITED STATES OF AMERICA *v.* HAMZA BENDELLADJ (A.K.A. "BX1")	Criminal Action No. 1:11-CR-557-AT-2



In short, Bendelladj is responsible for a loss amount of at least $100,000,000 dollars (200,000 cards x $500). *See* U.S.S.G. 2B1.1 Application Note 3(F)(i) ("In a case involving any unauthorized access device, loss . . . shall be not less than $500 per access device.").[55]

The tough business life of the hacker

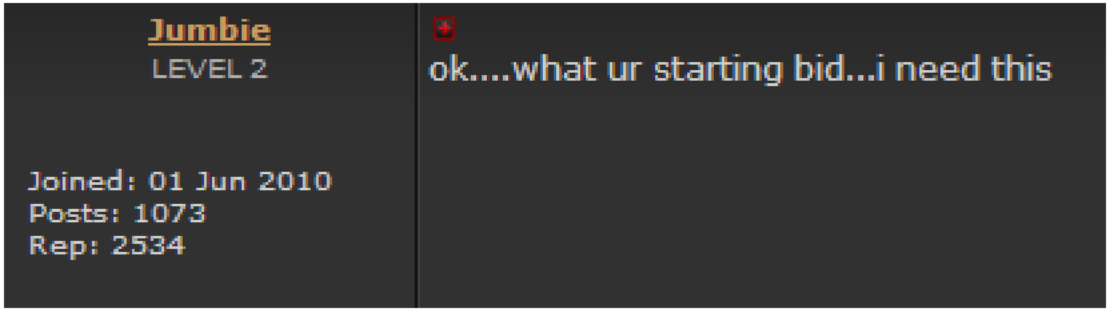


bx1
Guest

Info it have

CC NUMBER
EXP DATE
CVV
BILLING ADDRESS / SHIPPING ADDRESS
EMAIL - PASSWORD

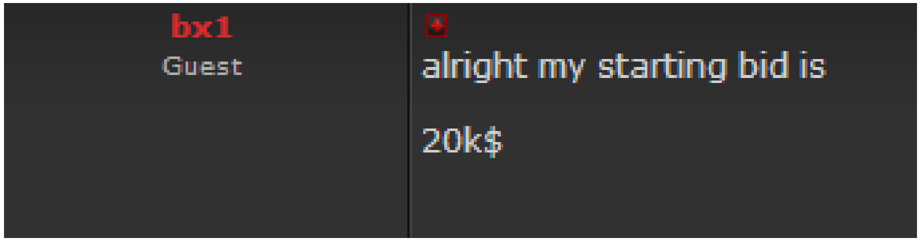
Sat Dec 03, 2011 3:13 am



Jumbie
LEVEL 2

Joined: 01 Jun 2010
Posts: 1073
Rep: 2534

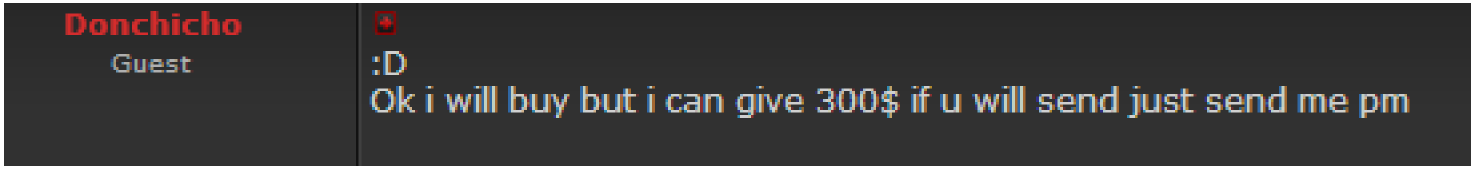
ok....what ur starting bid...i need this



bx1
Guest

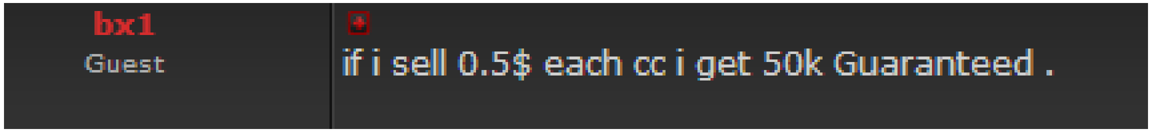
alright my starting bid is

20k$



Donchicho
Guest

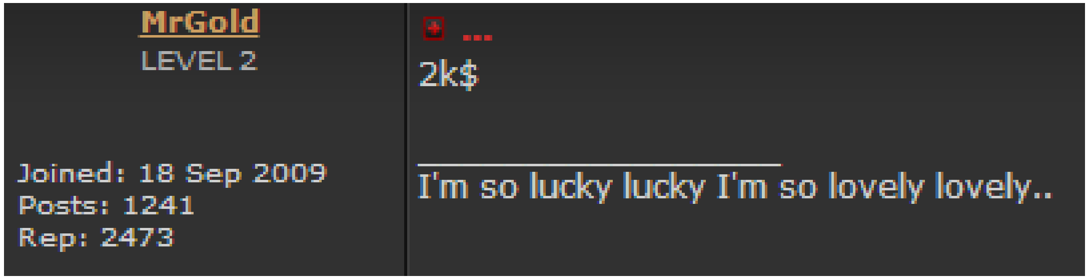
:D
Ok i will buy but i can give 300$ if u will send just send me pm



bx1
Guest

if i sell 0.5$ each cc i get 50k Guaranteed .

The tough business life of the hacker

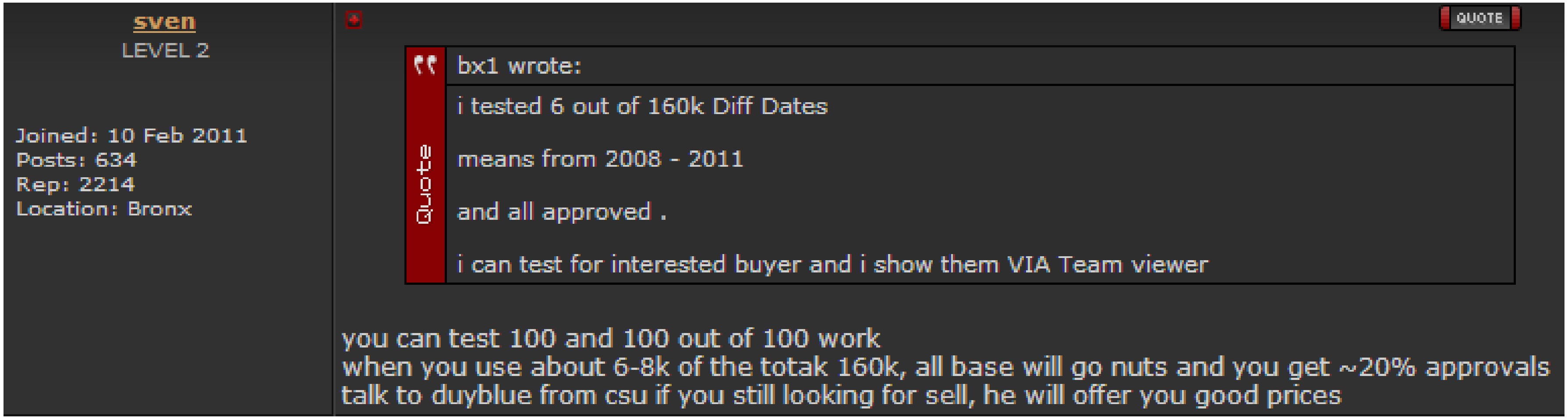


MrGold
LEVEL 2

Joined: 18 Sep 2009
Posts: 1241
Rep: 2473

2k$

I'm so lucky lucky I'm so lovely lovely..

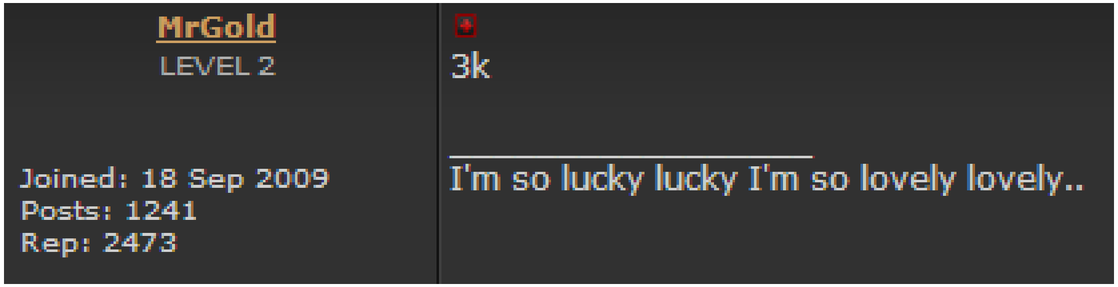


sven
LEVEL 2

Joined: 10 Feb 2011
Posts: 634
Rep: 2214
Location: Bronx

> bx1 wrote:
>
> i tested 6 out of 160k Diff Dates
>
> means from 2008 - 2011
>
> and all approved .
>
> i can test for interested buyer and i show them VIA Team viewer

you can test 100 and 100 out of 100 work
when you use about 6-8k of the totak 160k, all base will go nuts and you get ~20% approvals
talk to duyblue from csu if you still looking for sell, he will offer you good prices



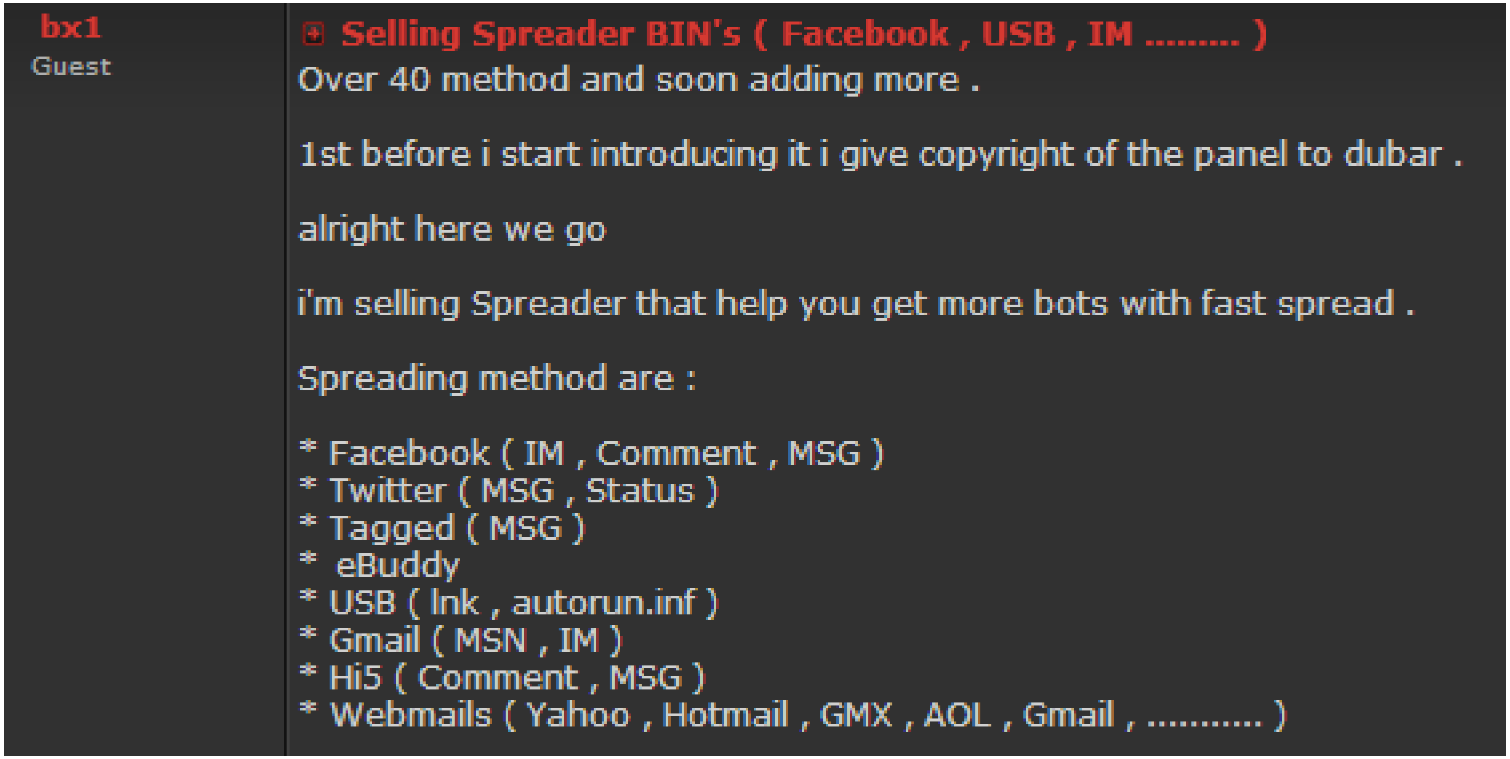
MrGold
LEVEL 2

Joined: 18 Sep 2009
Posts: 1241
Rep: 2473

3k

I'm so lucky lucky I'm so lovely lovely..

The tough business life of the hacker



bx1
Guest

Selling Spreader BIN's (Facebook , USB , IM ....)

Over 40 method and soon adding more .

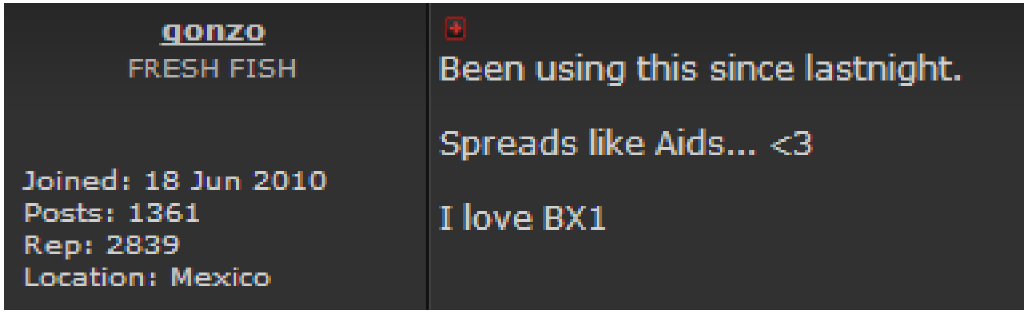
1st before i start introducing it i give copyright of the panel to dubar .

alright here we go

i'm selling Spreader that help you get more bots with fast spread .

Spreading method are :

* Facebook (IM , Comment , MSG)
* Twitter (MSG , Status)
* Tagged (MSG)
* eBuddy
* USB (lnk , autorun.inf)
* Gmail (MSN , IM)
* Hi5 (Comment , MSG)
* Webmails (Yahoo , Hotmail , GMX , AOL , Gmail , ...)



gonzo
FRESH FISH

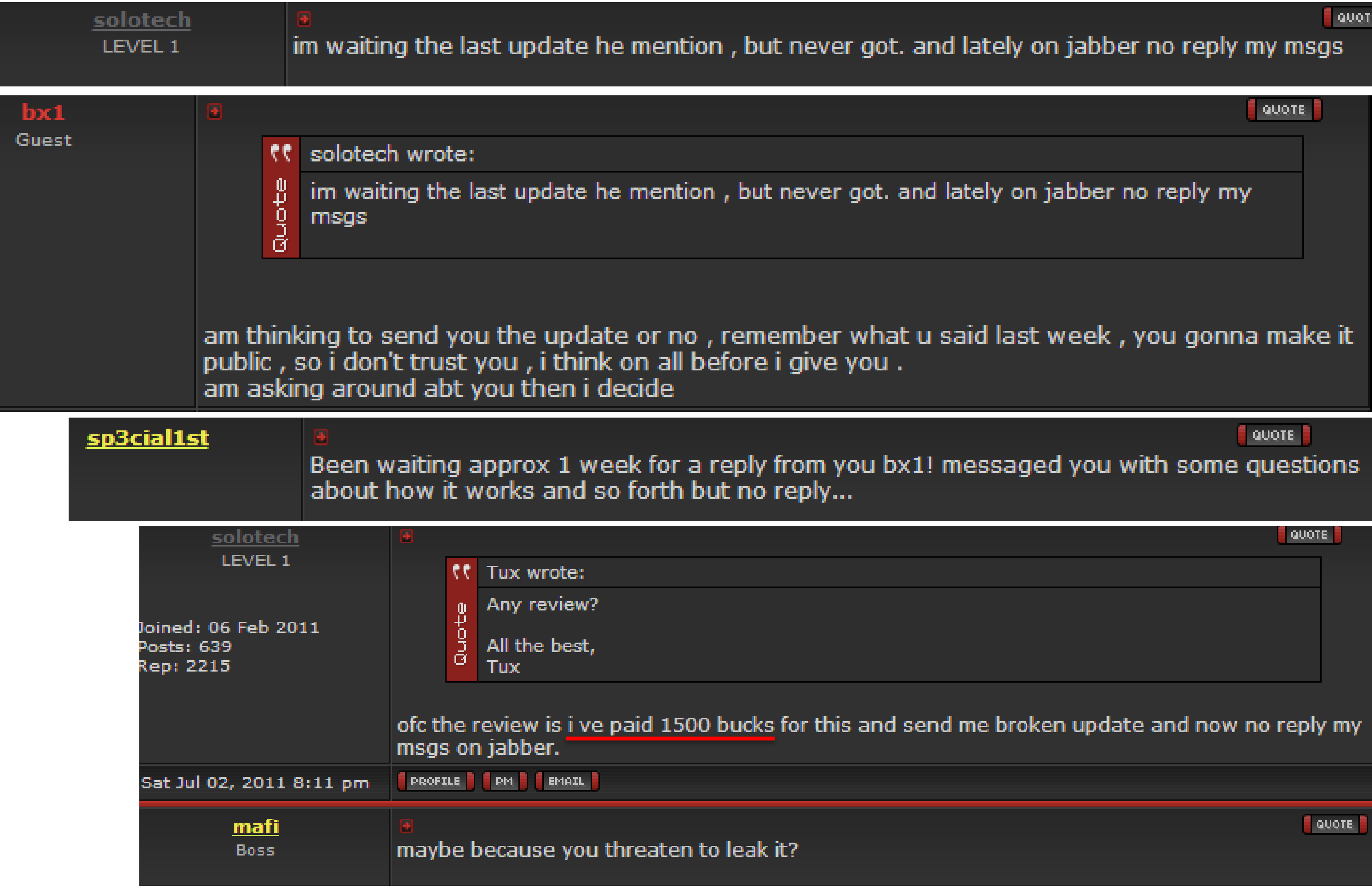
Joined: 18 Jun 2010
Posts: 1361
Rep: 2839
Location: Mexico

Been using this since lastnight.

Spreads like Aids... <3

I love BX1

The tough business life of the hacker



solotech
LEVEL 1

im waiting the last update he mention , but never got. and lately on jabber no reply my msgs

bx1
Guest

> solotech wrote:
>
> im waiting the last update he mention , but never got. and lately on jabber no reply my msgs

am thinking to send you the update or no , remember what u said last week , you gonna make it public , so i don't trust you , i think on all before i give you .
am asking around abt you then i decide

sp3cial1st

Been waiting approx 1 week for a reply from you bx1! messaged you with some questions about how it works and so forth but no reply...

solotech
LEVEL 1

Joined: 06 Feb 2011
Posts: 639
Rep: 2215

> Tux wrote:
>
> Any review?
>
> All the best,
> Tux

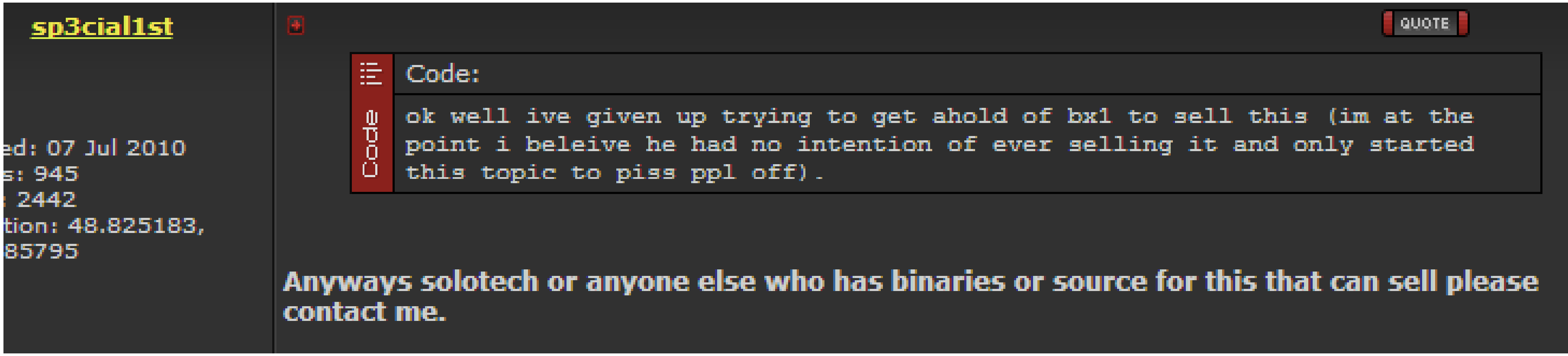
ofc the review is i ve paid 1500 bucks for this and send me broken update and now no reply my msgs on jabber.

Sat Jul 02, 2011 8:11 pm

mafi
Boss

maybe because you threaten to leak it?

2 months later… the issue remained unresolved



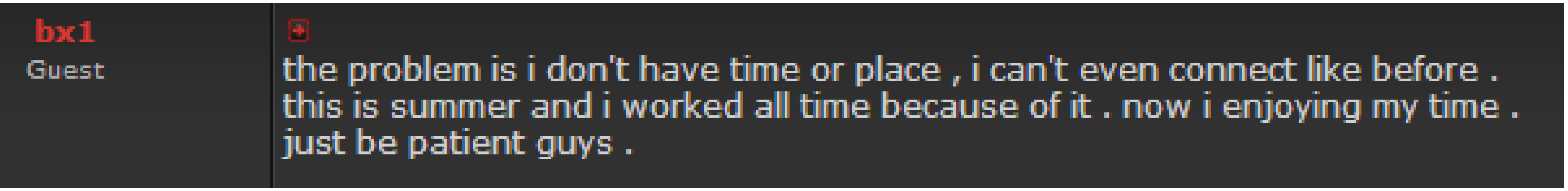
sp3cial1st

ed: 07 Jul 2010
s: 945
: 2442
tion: 48.825183,
85795

Code:

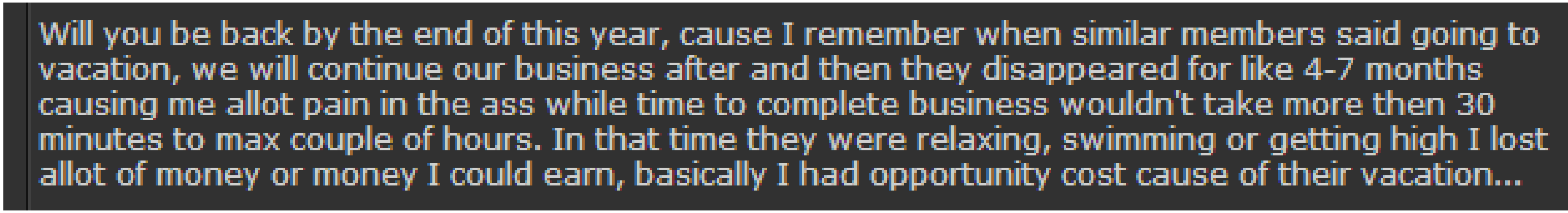
```
ok well ive given up trying to get ahold of bx1 to sell this (im at the
point i beleive he had no intention of ever selling it and only started
this topic to piss ppl off).
```

Anyways solotech or anyone else who has binaries or source for this that can sell please contact me.



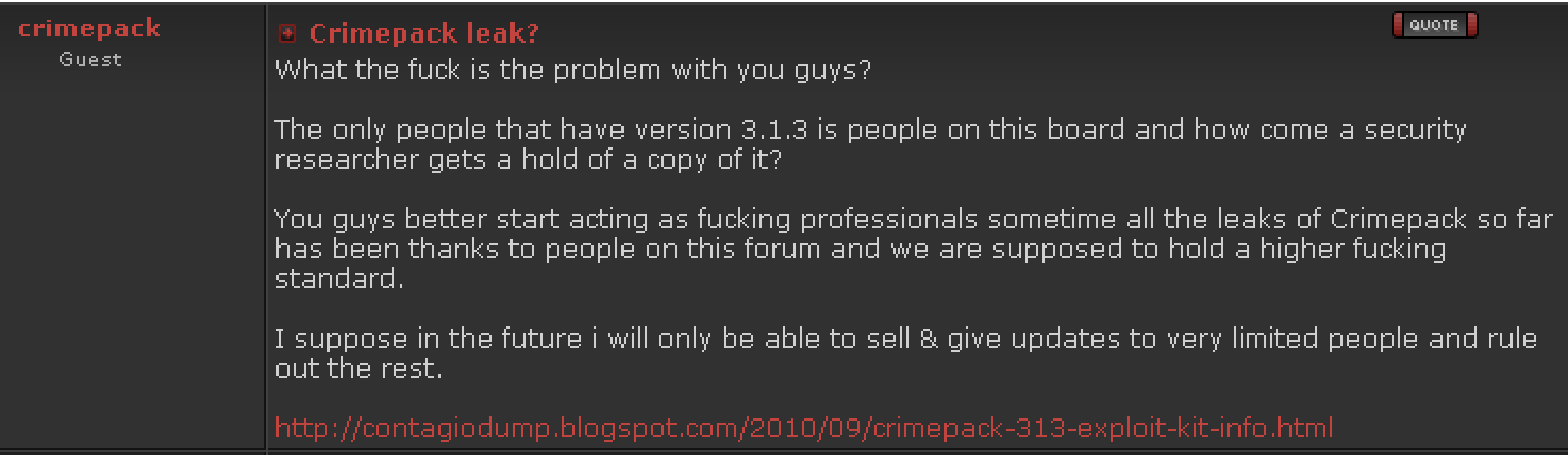
bx1
Guest

the problem is i don't have time or place , i can't even connect like before . this is summer and i worked all time because of it . now i enjoying my time . just be patient guys .



Will you be back by the end of this year, cause I remember when similar members said going to vacation, we will continue our business after and then they disappeared for like 4-7 months causing me allot pain in the ass while time to complete business wouldn't take more then 30 minutes to max couple of hours. In that time they were relaxing, swimming or getting high I lost allot of money or money I could earn, basically I had opportunity cost cause of their vacation...

Not a problem exclusive to bx1



Crimepack leak?

What the fuck is the problem with you guys?

The only people that have version 3.1.3 is people on this board and how come a security researcher gets a hold of a copy of it?

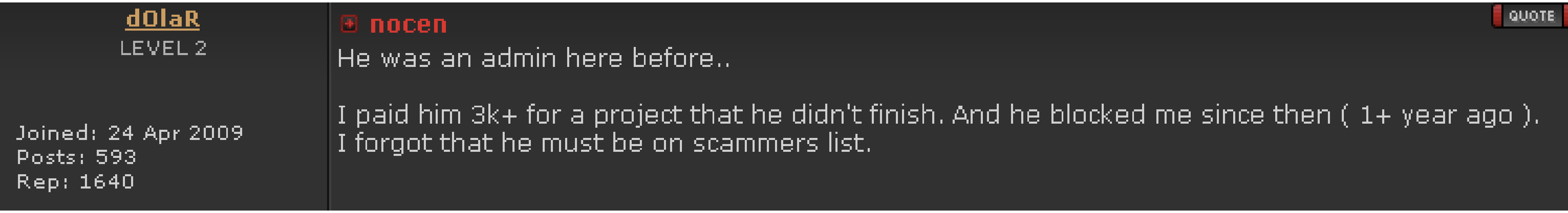
You guys better start acting as fucking professionals sometime all the leaks of Crimepack so far has been thanks to people on this forum and we are supposed to hold a higher fucking standard.

I suppose in the future i will only be able to sell & give updates to very limited people and rule out the rest.

http://contagiodump.blogspot.com/2010/09/crimepack-313-exploit-kit-info.html

Scammers' reports

- 151 complaints over 4 years
- Equals 44% of newly admitted members



d0laR

LEVEL 2

Joined: 24 Apr 2009
Posts: 593
Rep: 1640

nocen

He was an admin here before..

I paid him 3k+ for a project that he didn't finish. And he blocked me since then (1+ year ago).
I forgot that he must be on scammers list.

ALICE, I WANT YOU TO INTERVIEW A JOB CANDIDATE. LET ME KNOW WHAT YOU THINK.
www.dilbert.com
scottadams@aol.com
WHY DID YOU LEAVE YOUR LAST JOB?
I PUNCHED MY BOSS.
©2008 Scott Adams, Inc./Dist. by UFS, Inc.
HE'S EXACTLY WHAT WE NEED.

Questions & ideas?
benoit.dupont@umontreal.ca