RSAConference2019
Asia Pacific & Japan
Singapore | 16–18 July | Marina Bay Sands

BETTER.

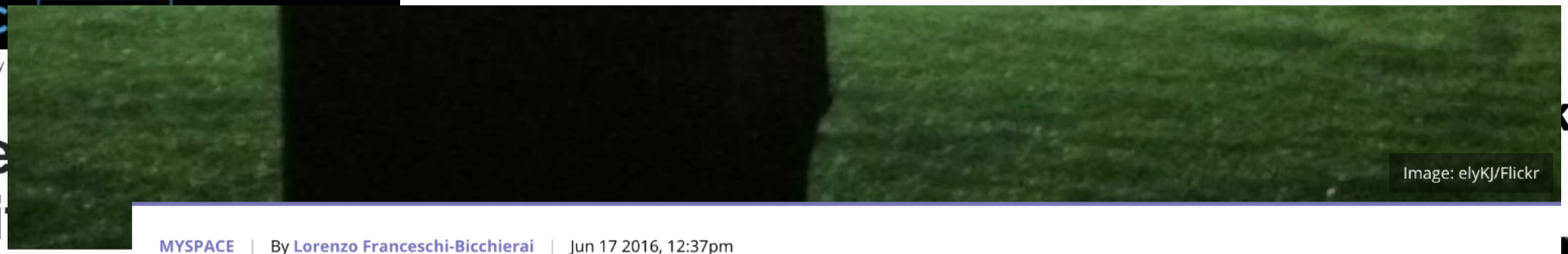
SESSION ID: FLE-R03

Tessa88: Uncovering the True Identity of the Notorious Hacker

Andrei Barysevich

Director of Advanced Collection
Recorded Future
@DeepSpaceEye

tessa88 in the media



MYSPACE | By Lorenzo Franceschi-Bicchierai | Jun 17 2016, 12:37pm

This Is The Hacker Allegedly Behind The LinkedIn and MySpace Megabreaches

Who is Tessa88, the other hacker who's spreading and selling hacked passwords stolen from your social networks?

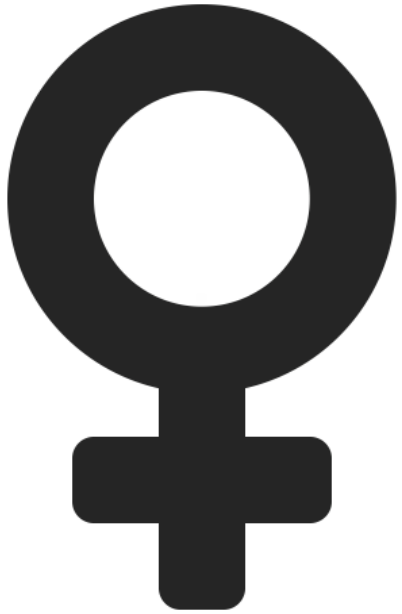
SHARE TWEET

The Actor`s Indicators Known Before Investigation

- Usernames:
  - tessa88
  - stervasgoa
  - jannet93
- Jabbers:
  - tessa88@exploit[.]im
  - tessa88@xmpp[.]jp
  - mrfreeman777@xmpp[.]jp
  - darksideglobal@exploit[.]im
- Email addresses:
  - firetessa@yahoo[.]com
- Twitter:
  - @firetessa
- ICQ:
  - 740455
- Website:
  - darkside.global.deer[.]io
- Bitcoin wallet:
  - 1AbMLfZPB59H6gwqWHnA9bnUQt3JB2gAoC

Female? Male? Two Different People?

- tessa88
- stervasgoa [bitch from Goa]
- jannet93

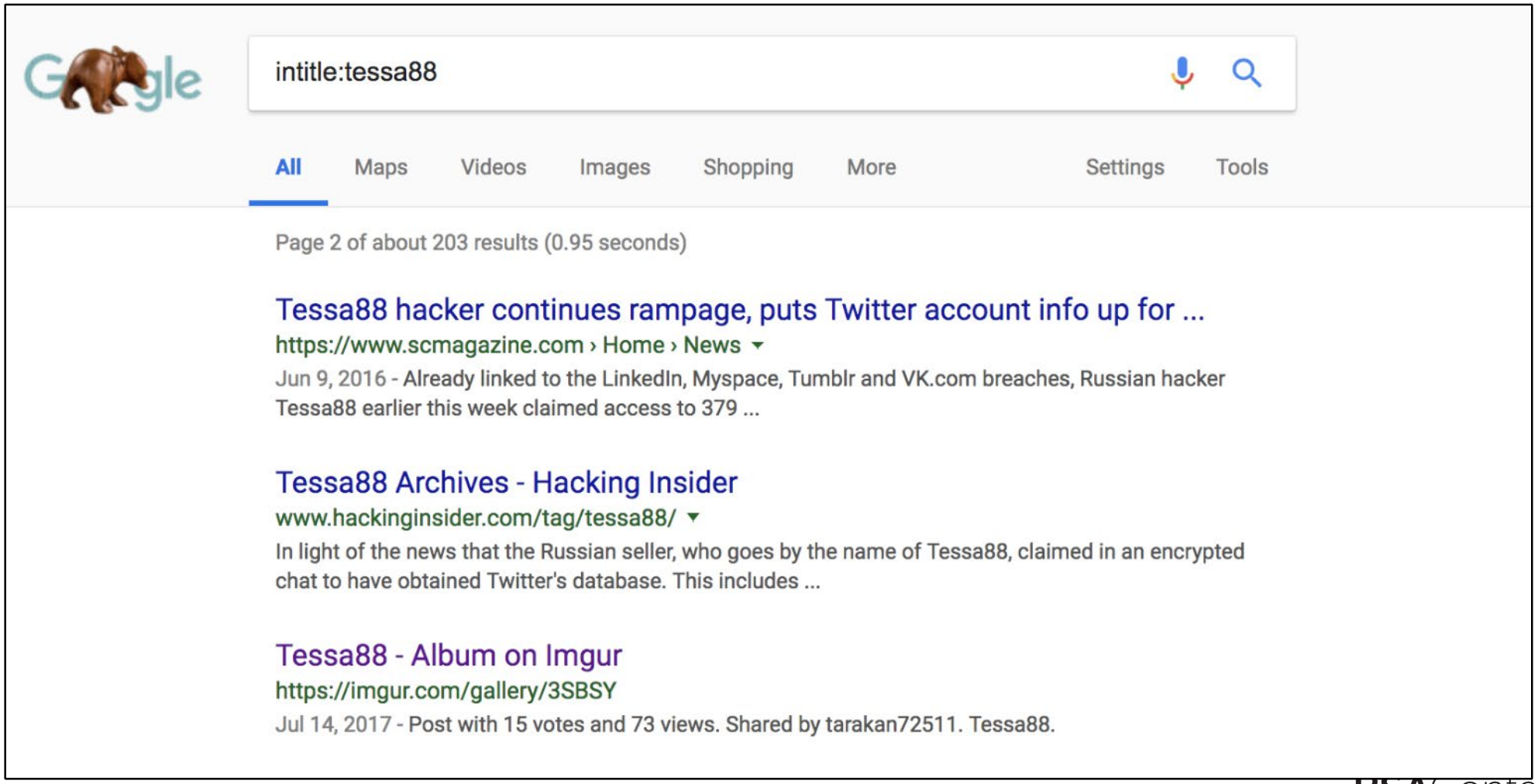


TraX - a Member of 0Day Forum Claimed That He Met tessa88 in Person, the Actor is a Man

TraX`s Post in Recorded Future Platform Saying That tessa is a Man

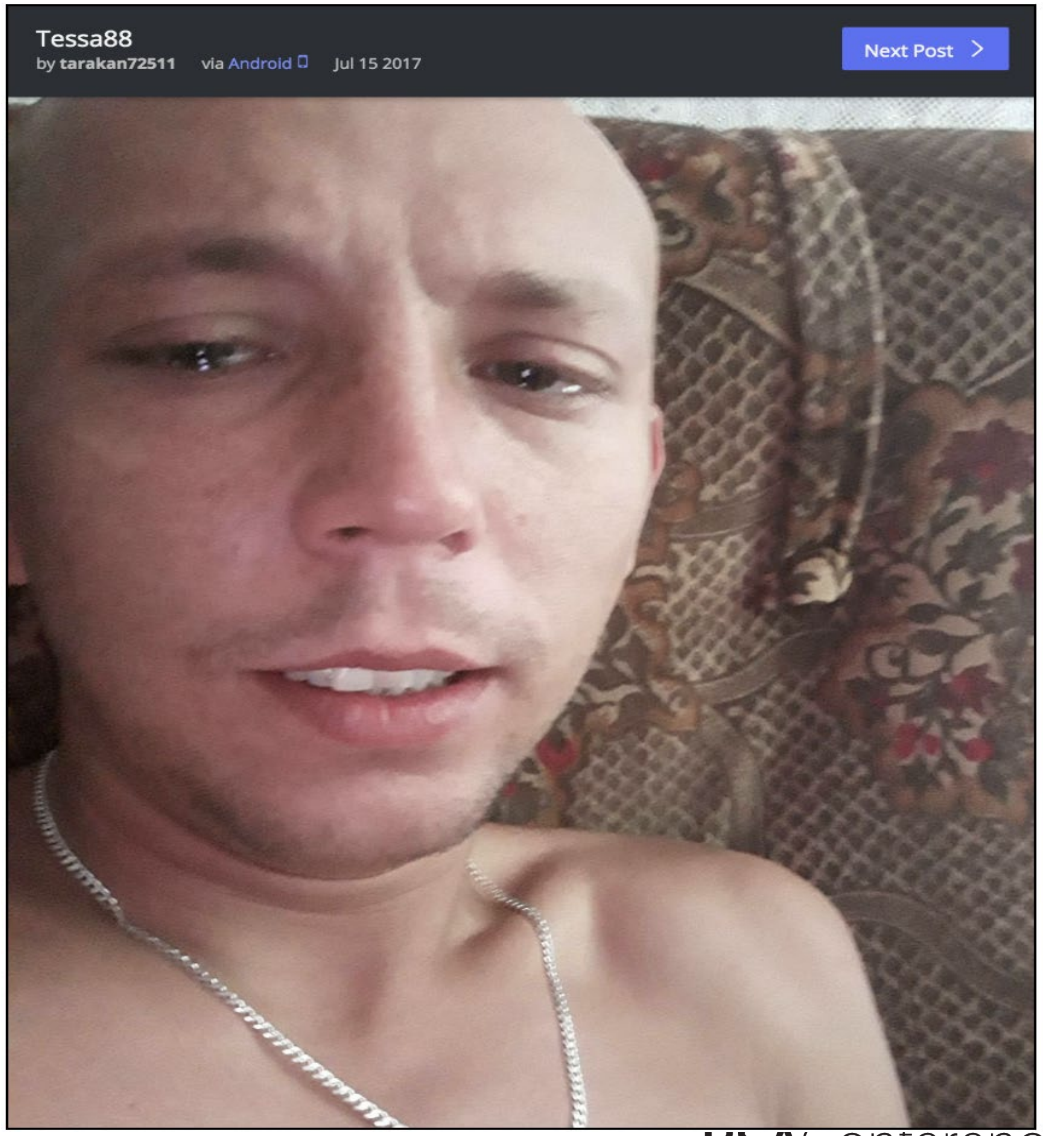
OSINT for “tessa88” Revealed the Imgur Account “tarakan72511”

We used Google Advanced Search using a combination “intitle:tessa88”



We Identified an Alleged Photo of tessa88

The user tarakan72511 posted a photo of the man titled “Tessa88” in 2017, whose body type and hairstyle is similar to the individual depicted in the picture posted by TraX on 0Day forum.

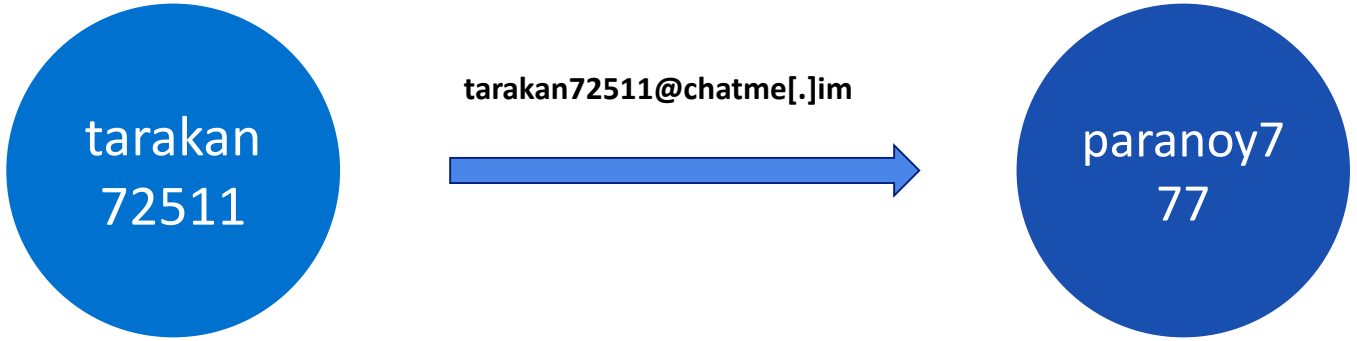



tarakan
72511

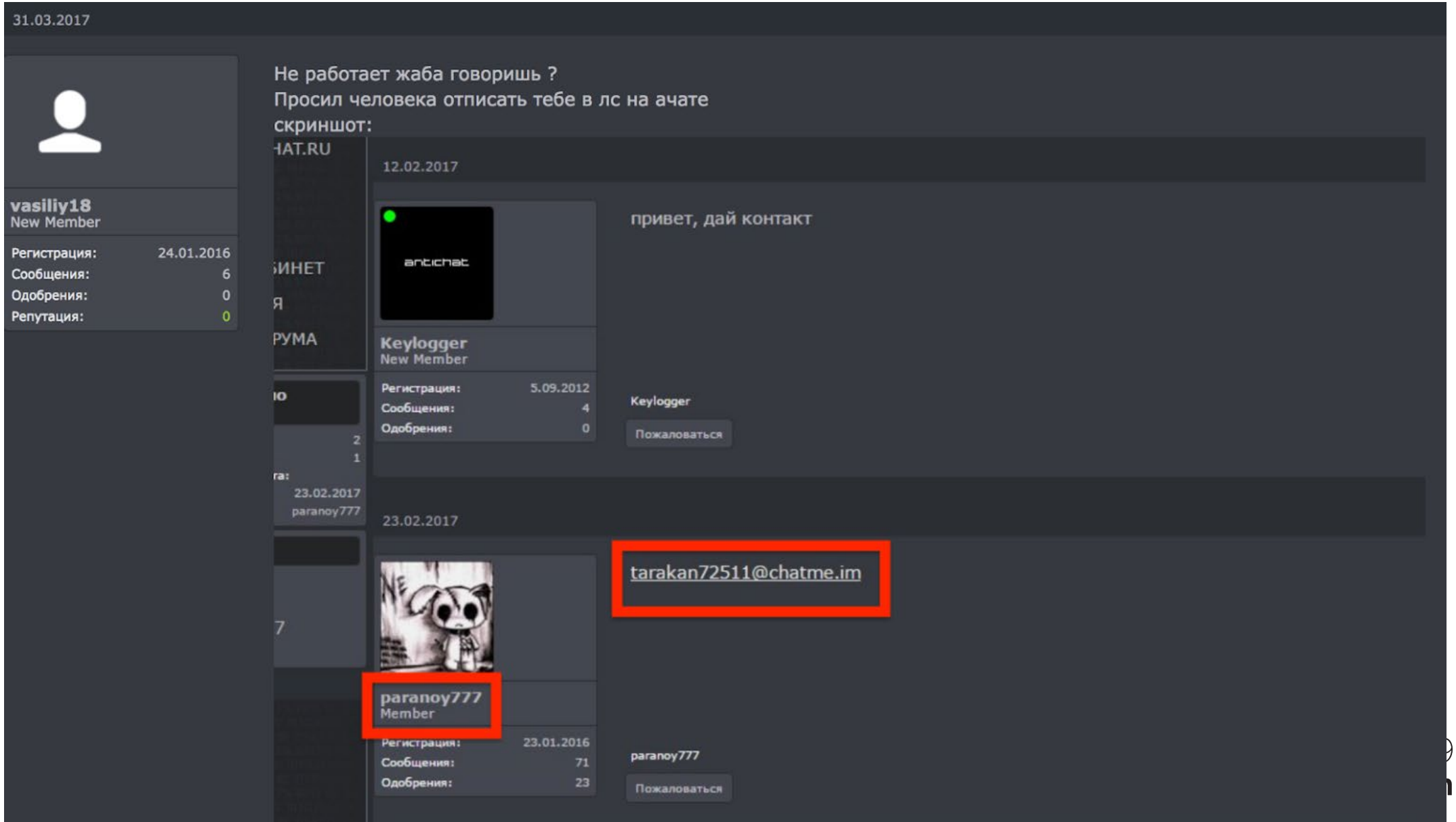
Connection Between Threat Actors tessa88 and paranoy777

- The username “tarakan72511” likely belongs to the actor paranoy777, who used the Jabber account **tarakan72511@chatme[.]im** on several underground forums in 2017.

- Recorded Future earlier investigated the activity of paranoy777. This actor, as well as tessa88, had previously been selling stolen email databases from the large social media and technology companies. The actors have not been observed corresponding with one another openly on dark web forums.


tarakan
72511
tarakan72511@chatme[.]im
paranoy7
77

paranoy777 Used the jabber “tarakan72511@chatme[.]im” on Antichat and Other Forums

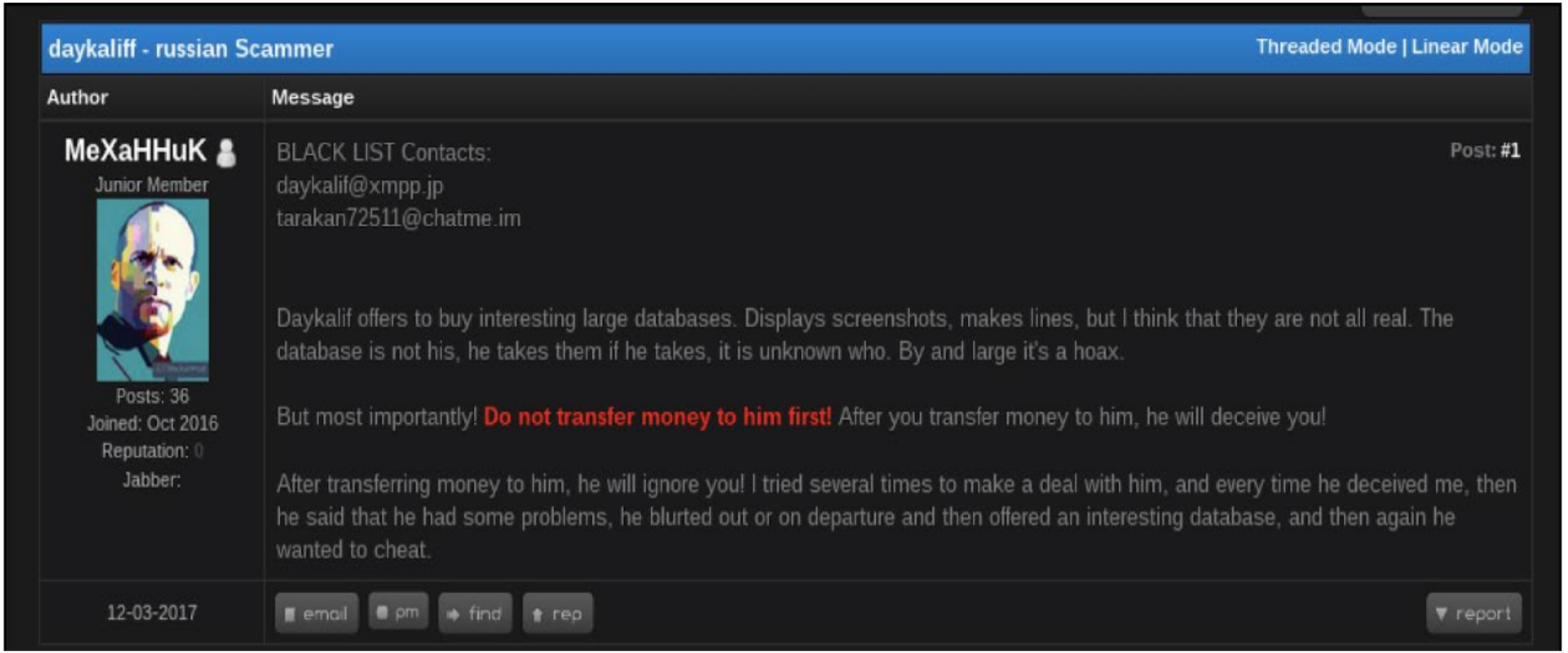


Connection Between the Actors paranoy777 and daykalif

Underground forum search for the mentioned above jabber account **tarakan72511@chatme[.]im** revealed a claim by the actor **MeXaHHuK**, who posted on 0Day forum that **daykalif** is a Russian-speaking scammer involved in the sale of large databases, and used the Jabber accounts **daykalif@xmpp[.]jp** and **tarakan72511@chatme[.]im**.

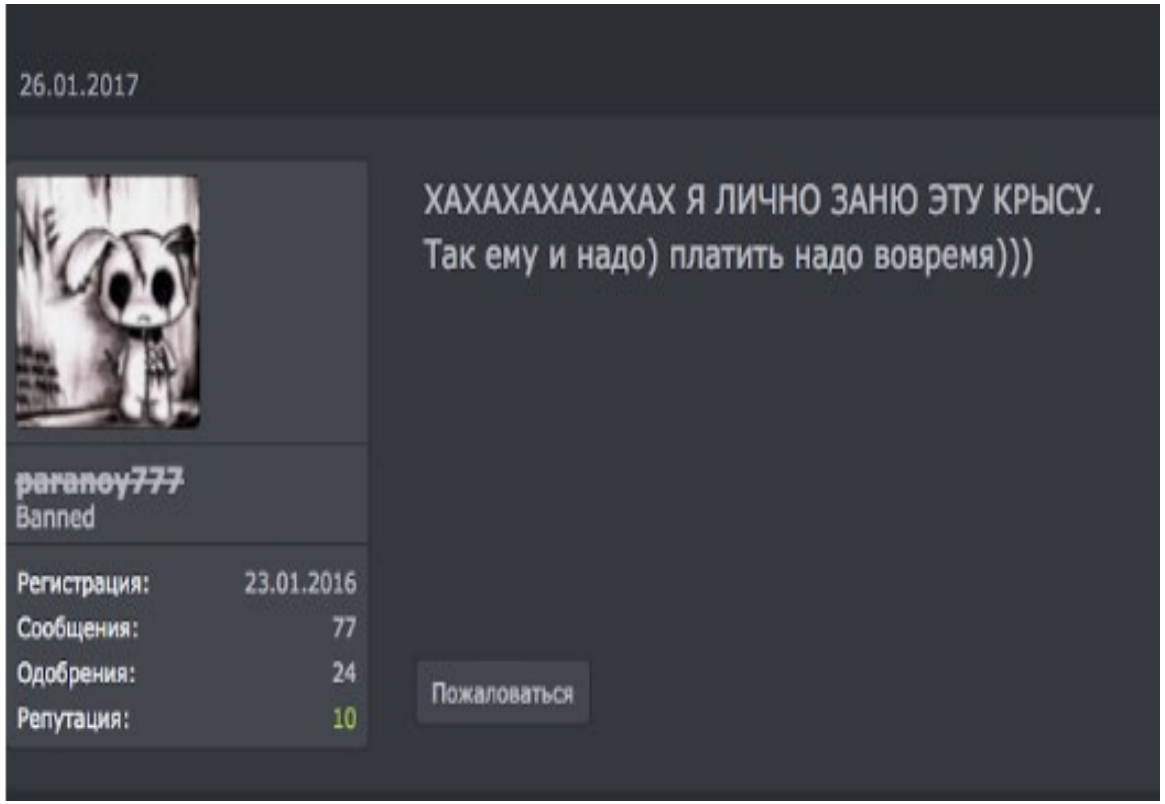
These facts mean that **paranoy777** and **daykalif** might be the same individual.

MeXaHHuK`s Post on 0DAY Accused daykalif of Scamming



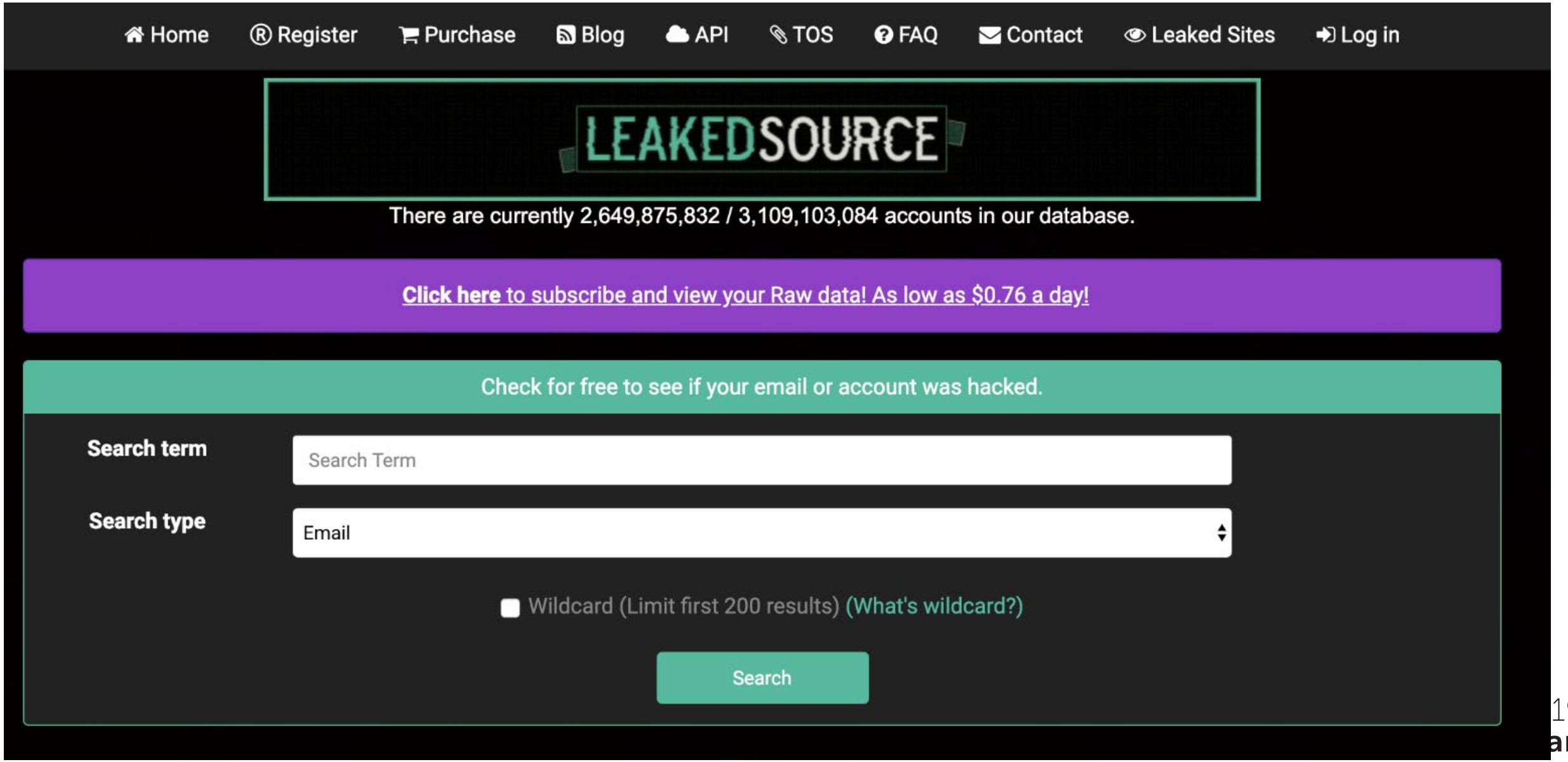

tarakan
72511
tarakan72511@chatme[.]im
paranoy7
77
daykalif@xmpp[.]jp
tarakan72511@chatme.im
daykalif

Connection Between the Actors paranoy777 and daykalif

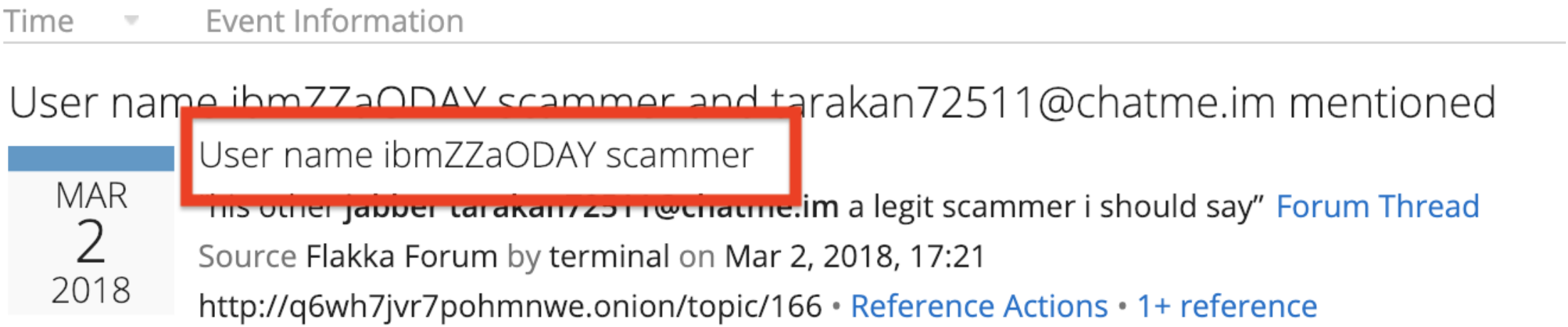


- According to the media, **daykalif** sold the Rambler and Last.fm databases to the currently-defunct LeakedSource in September 2016.
- On January 26, 2017, during the discussion of recent takedown of the **LeakedSource** by the FBI, between members of the Antichat forum, **paranoy777 admitted** that he was happy to see the website being seized
  "I known this "rat" personally, he deserved it. He should have paid on time."
- Another evidence that **paranoy777** and **daykalif** are the same person who sold stolen databases to LeakedSource

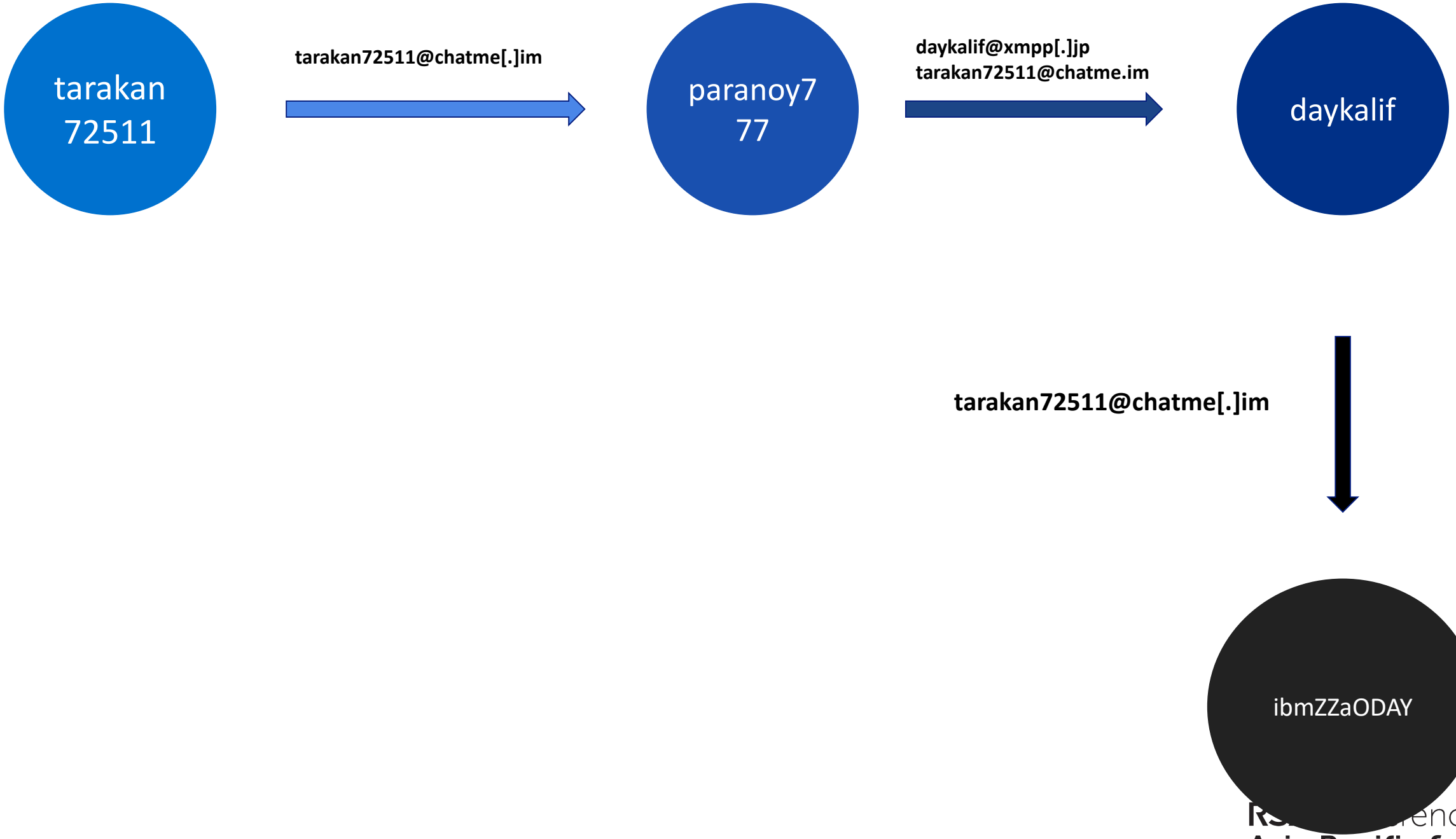
LeakedSource is Back



ibmZZa0DAY, Another Alias of tarakan72511, paranoy777, and daykalif

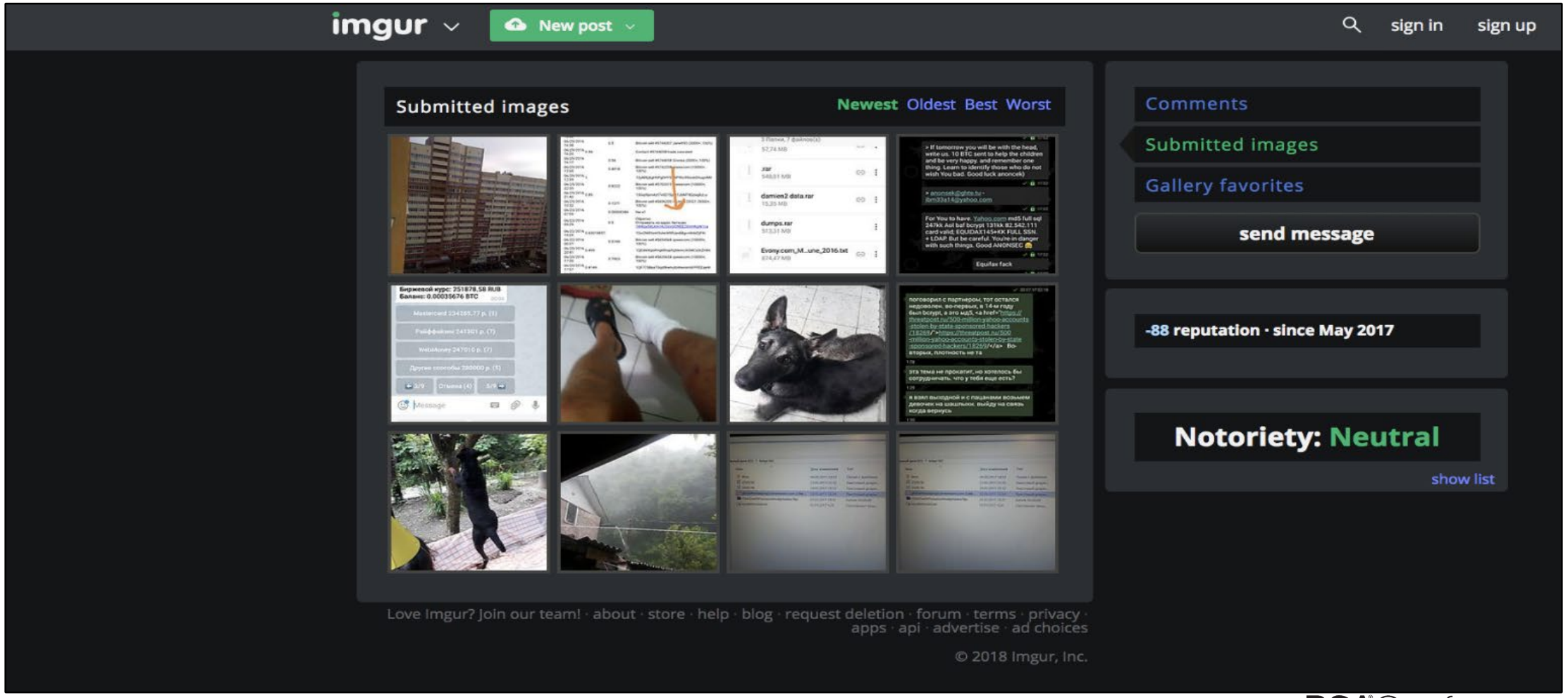


tarakan72511@chatme[.]im belongs to **ibmZZa0DAY**, a member of the Flakka forum. The actor used the same jabber and was also accused of scamming.


tarakan
72511
tarakan72511@chatme[.]im
paranoy7
77
daykalif@xmpp[.]jp
tarakan72511@chatme.im
daykalif
tarakan72511@chatme[.]im
ibmZZaODAY

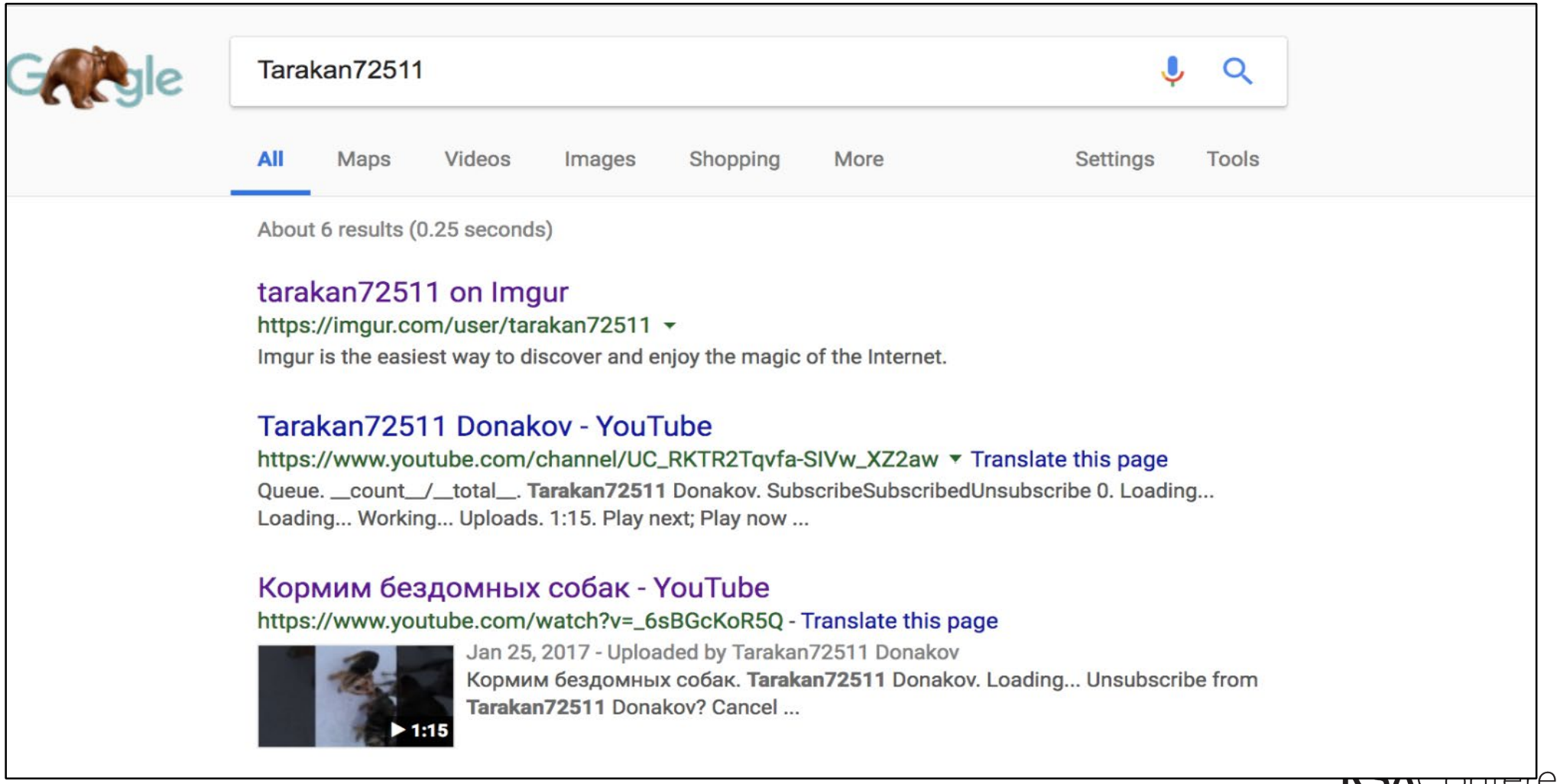
Analysis of tarakan72511`s Imgur Account

The Imgur account also revealed that the actor is an avid dog-lover



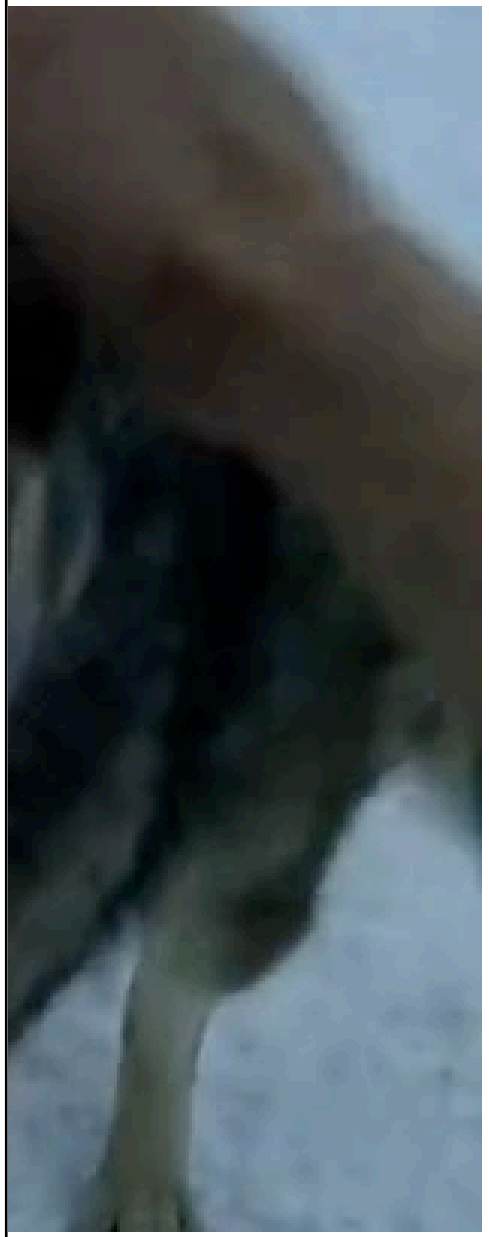
Tarakan72511`s YouTube video

OSINT for tarakan72511 revealed the YouTube user Tarakan72511 Donakov

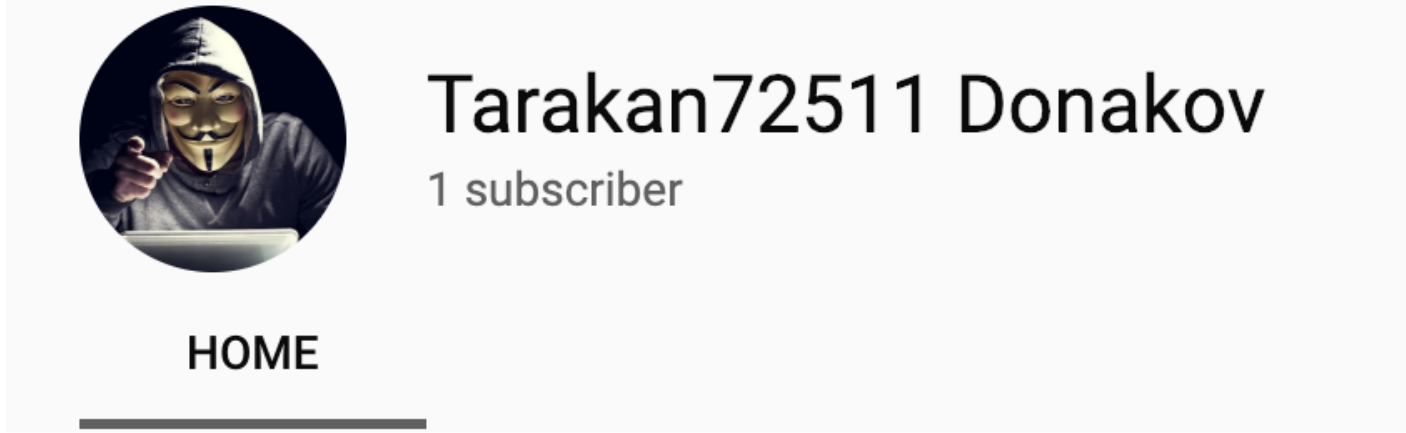


Tarakan72511 Donakov`s Video Showing Two Individuals Feeding Dogs

- The two individuals feeding the stray dogs in the video saying that they are residing in Penza, Russia.
- The vehicle make is Mitsubishi with the license plate “K 652BO 58.” (we confirmed, that the car was bought by Donakov M.V on December 18, 2016).



Mitsubishi License Plate “K 652BO 58” and a Guy Fawkes Mask



- On the 00:56 second, a Guy Fawkes mask seen on the video. A similar mask used as an avatar of the Tarakan72511 Donakov YouTube profile and also worn by the person in the image shared by TraX.

- OSINT for “Донаков” (Donakov) from Penza/Пенза revealed that someone Донаков M.B. committed several crimes in Yaroslavl and Penza, Russia, including a car theft and traffic accident that happened while driving “Mitsubishi Lancer” in 2017.

- Prior moving to Penza in 2014, Donakov Maksim Vladimirovich/Донаков Максим Владимирович resided in Yaroslav, were mentioned in several articles on SuDact, the largest non-governmental Russian website of judicial records. According to the website, Donakov spent several years in prison prior to the car accident in 2017.

Recorded Future

Court Records for Donakov M.V. (Донаков М.В.)

Донаков М.В.

Участник судебных дел

Последние документы:

1. **Решение от 19 октября 2017 г. по делу № 2-1756/2017**
   Первомайский районный суд г. Пензы (Пензенская область) - Гражданские и административные
   Суть спора: 2.145 - Иски о возмещении ущерба от ДТП (кроме увечий и смерти кормильца)

2. **Постановление от 13 сентября 2017 г. по делу № 5-587/2017**
   Ленинский районный суд г. Пензы (Пензенская область) - Административные правонарушения

3. **Апелляционное постановление от 27 марта 2014 г. по делу № 22-423/2014**
   Ярославский областной суд (Ярославская область) - Уголовное

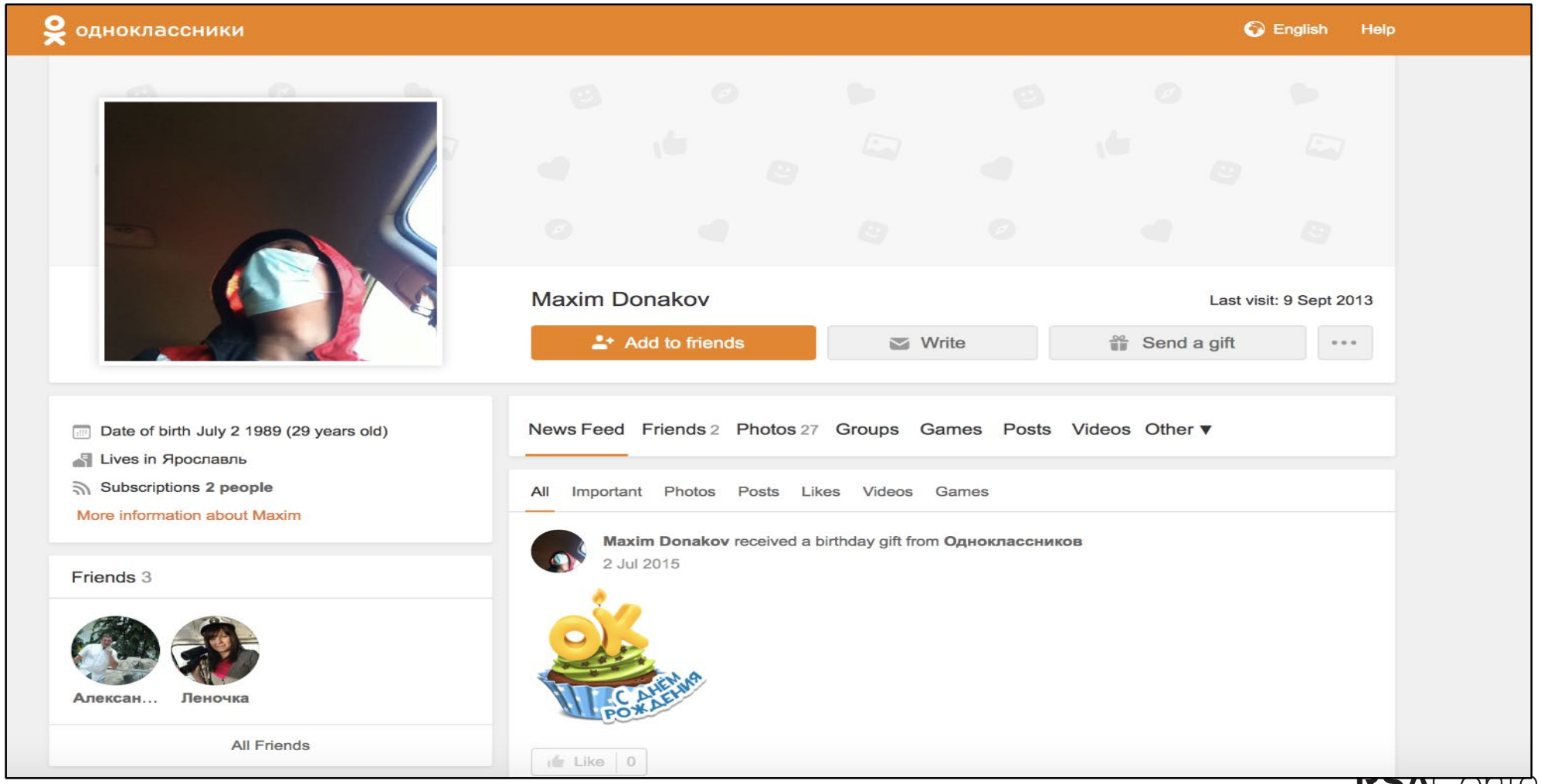
4. **Приговор от 20 февраля 2014 г.**
   Кировский районный суд г. Ярославля (Ярославская область) - Уголовное

- OSINT for Maxim Donakov revealed several profiles in the Russian social media Odnoklassniki. The first profile belongs to a man residing in Yaroslavl and who was born on July 2, 1989.

Recorded Future

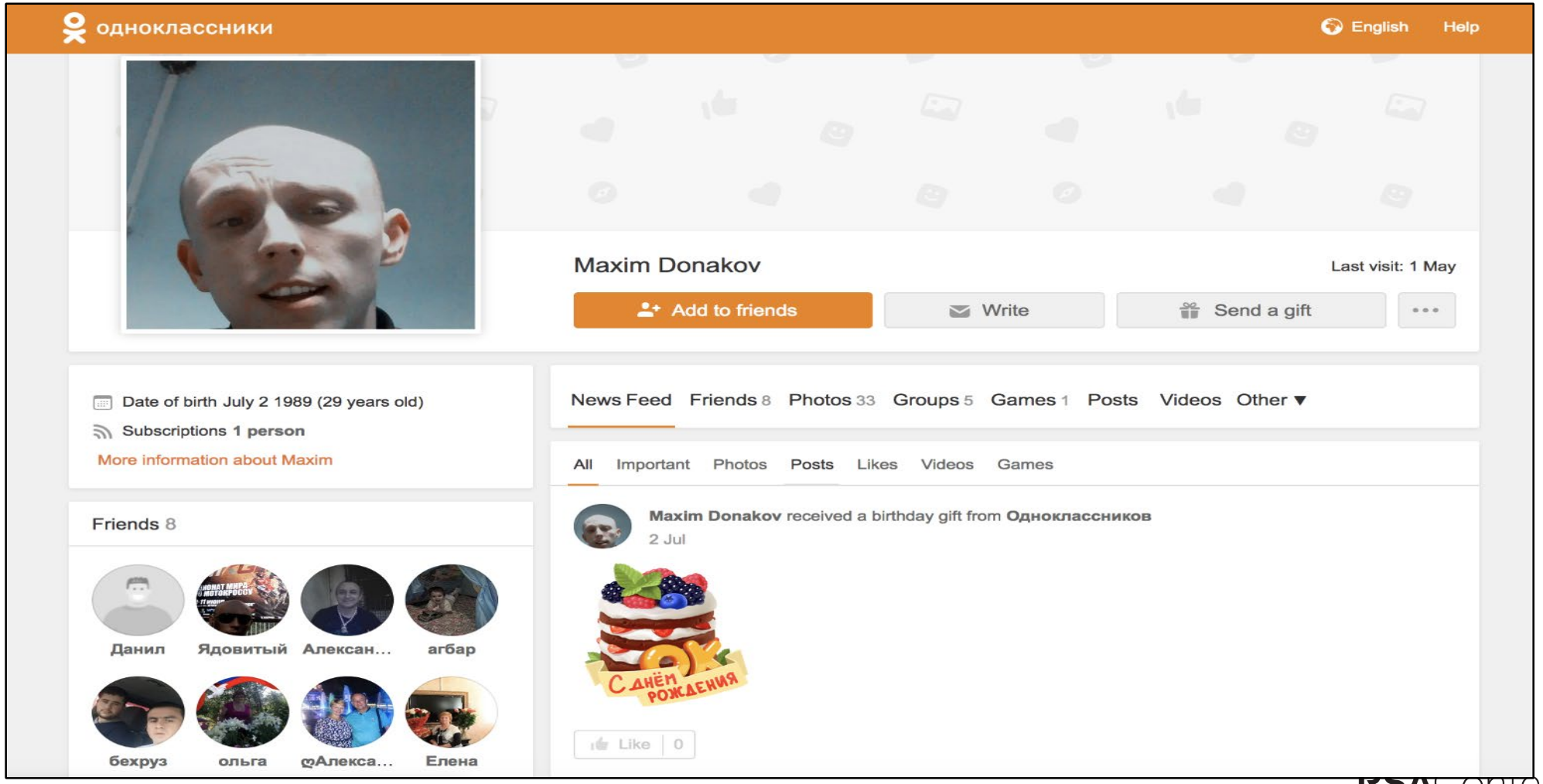
The 1st Donakov`s Odnoklassniki Profile

This profile indicates his date of birth July 2, 1989 and residence in Yaroslavl, Russia



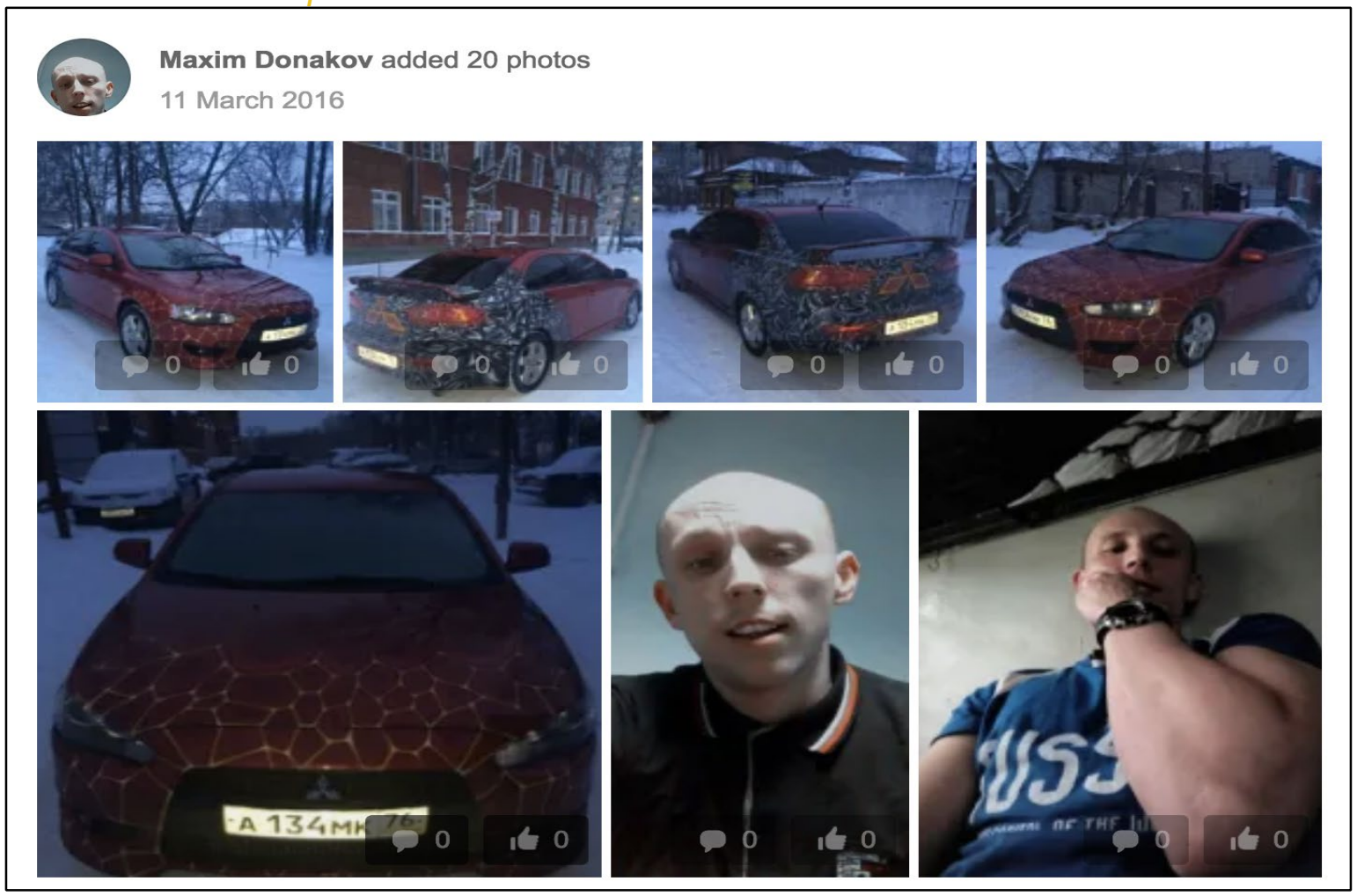
M.Donakov`s Odnoklassniki Profile #2 (OK.RU)

Date of birth - July 2, 1989

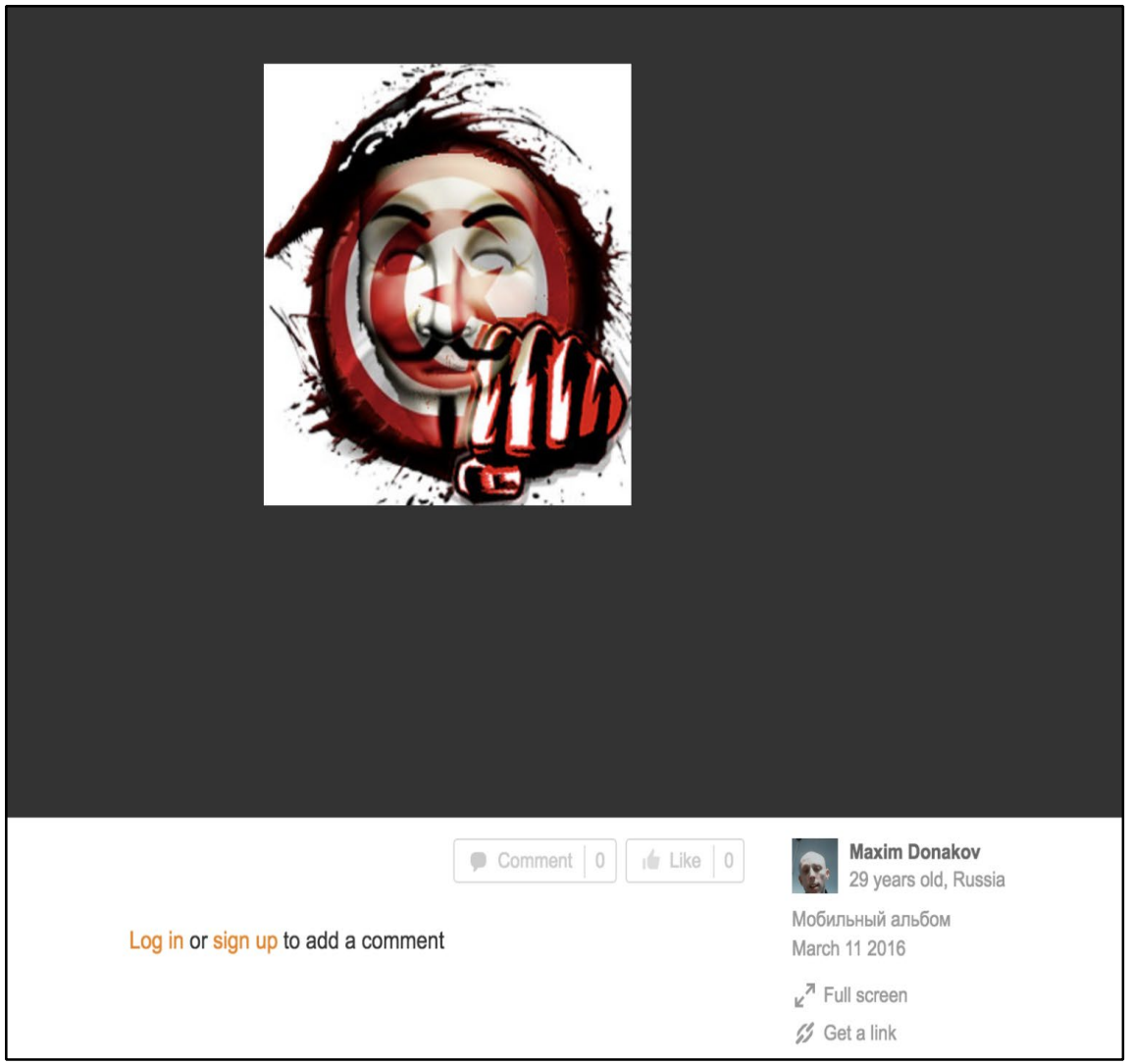


Photos of Donakov and Mitsubishi Lancer on the 1st OK.RU

Posted images depict the same individual seen in the Imgur image from tarakan72511, and Mitsubishi Lancer with the license plate "A 134MK 76" mentioned in the court records



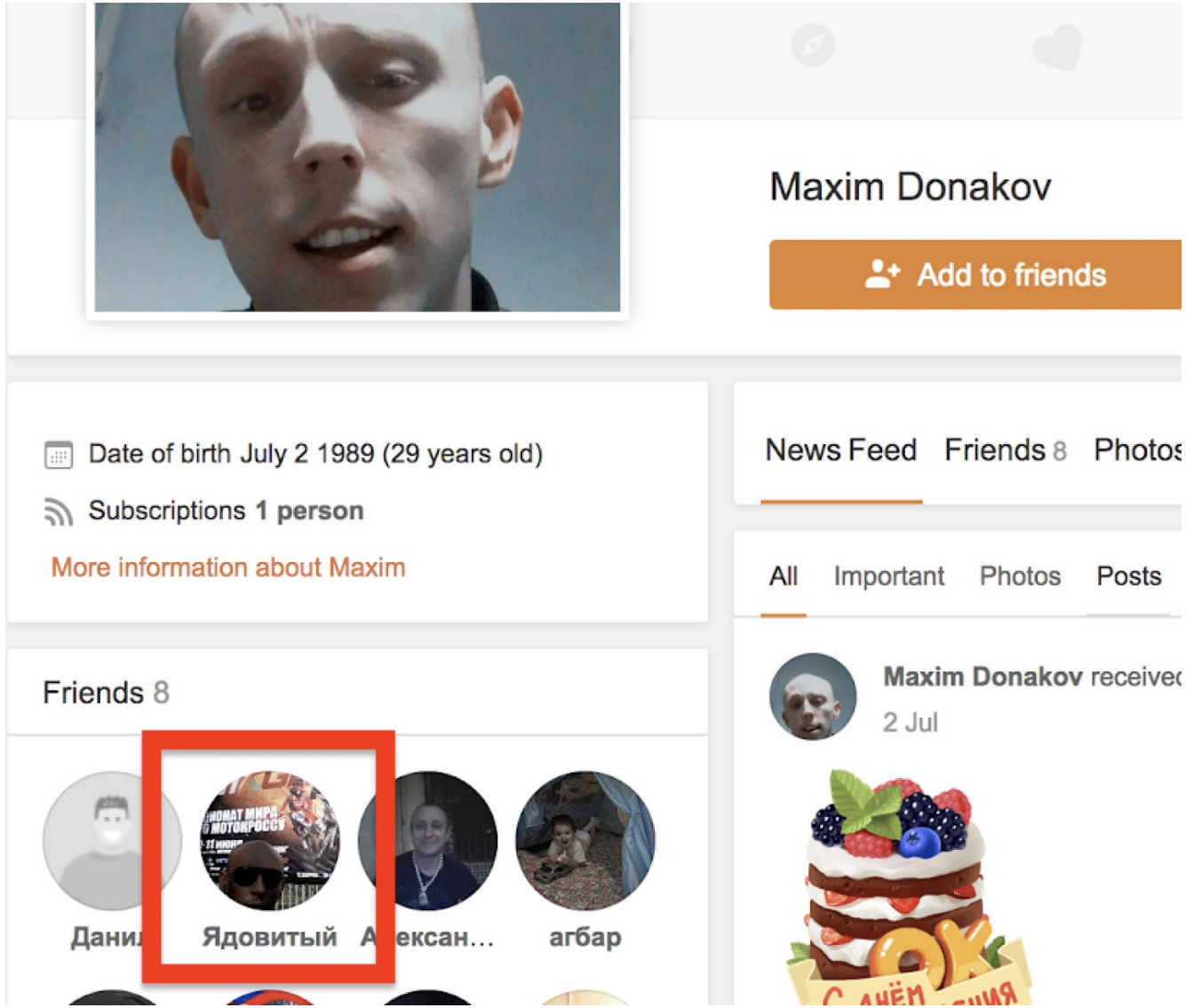
The 2nd OK.RU Profile Contains an Image of the Avatar Used by tessa88 on Multiple Underground Forums



- The analysis of the second Odnoklassniki profile revealed that it was linked to another profile created under the username “Ядовитый Таракан” (Yadovitiy Tarakan/Toxic cockroach) who is allegedly residing in Pervomaysk, Ukraine.
- The profile photo of the person depicted on it resembles Donakov Maxim very closely. Pervomaysk is Maxim Donakov `s real place of birth. We assess with a high degree of confidence that this profile also belongs to Donakov Maxim.

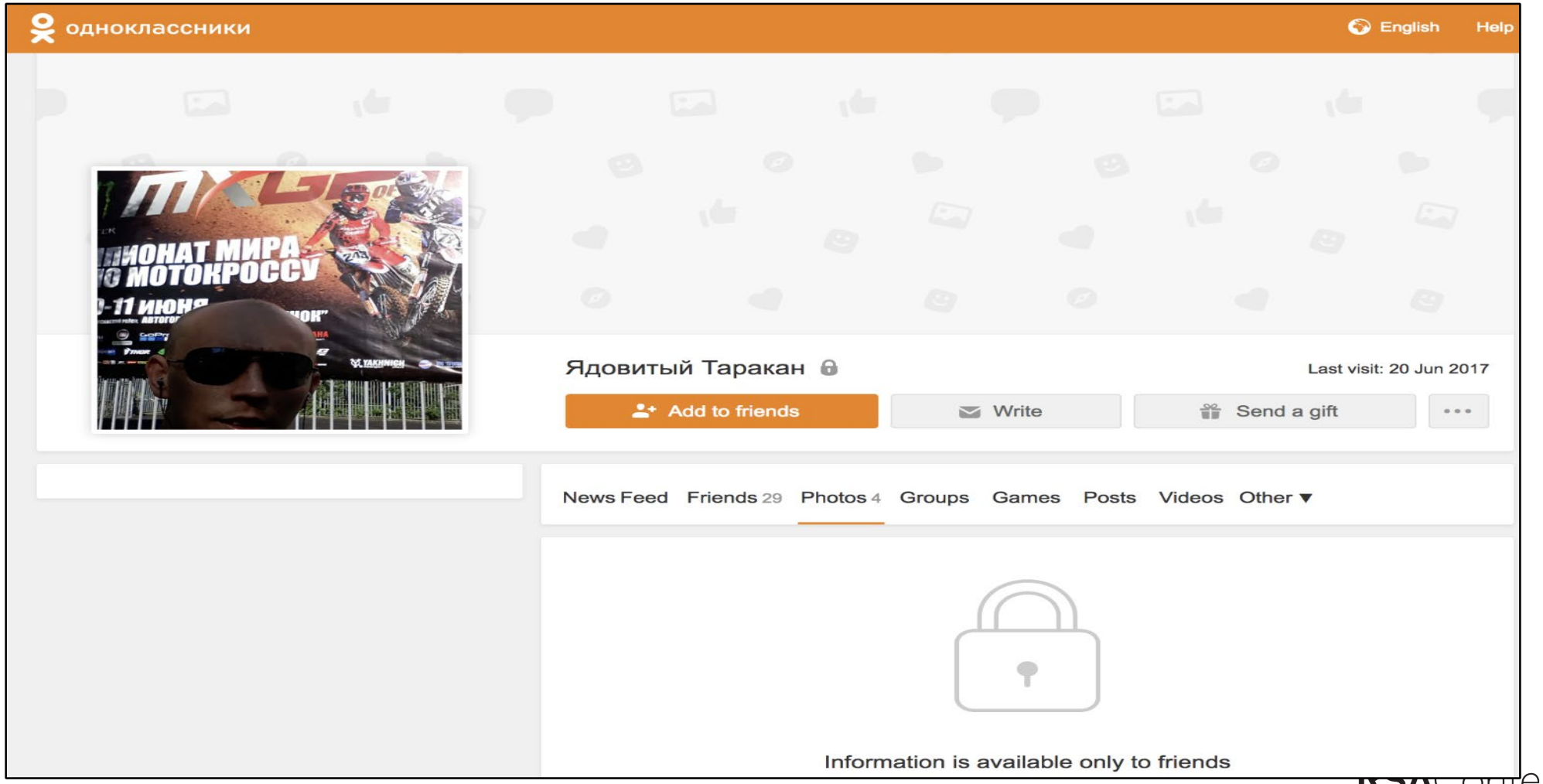
Recorded Future

The Third OK Profile Identified



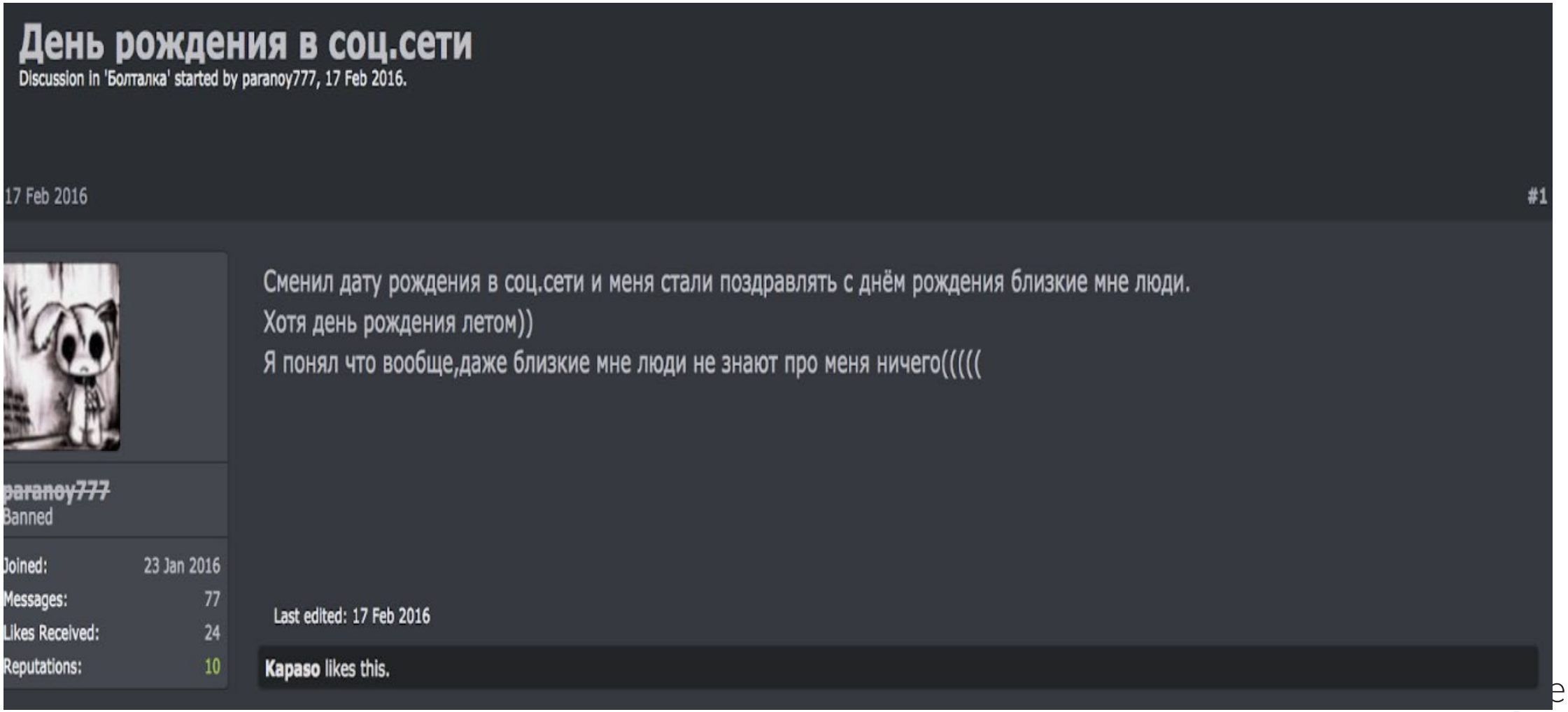
The 3rd Donakov`s OK.RU Profile Under the Username “Ядовитый Таракан”

The image of the individual resembles Donakov



Another Evidence That paranoy777 is Donakov

On February 17, 2016, paranoy777 mentioned on Antichat forum that his real date of birth is in summer (as well as Donakov`s)



tarakan 72511

tarakan72511@chatme[.]im

paranoy7 77

daykalif@xmpp[.]jp
tarakan72511@chatme.im

daykalif

tarakan72511@chatme[.]im

ibmZZaODAY

Additional Evidence That paranoy777 is Donakov

Coincidentally, the initial activity of the second OK.RU profile for Maxim Donakov was detected on November 26, 2015, which is the same day the user "khaym," registered on forum Exploit.

Connection Between the Actors paranoy777 and khaym

Insikt Group has confirmed earlier that “khaym” is another moniker used by paranoy777, who was banned on Exploit forum because of scamming. The actor used the following jabber accounts on the forum:

- khaym@exploit[.]im
- Bruno123123@yax[.]im
- demigrooop@exploit[.]im

- Sources confirmed that Maxim (Maksim) Donakov is a real person with a real date of birth July 2, 1989. He conducted several crimes in Yaroslavl and Penza, including vehicle theft and traffic accident.

- The existence of several profiles can be explained with his arrest. His last visit to the 2nd OK.RU profile was on September 9, 2013. The 1st profile was started in November 2015.

- According to the information on SuDact website, Donakov was released under police supervision but was then imprisoned after committing another crime in 2014.

Recorded Future

M.Donakov`s Passport Photo

M. Donakov`s passport photo greatly resembles the alleged photo of tessa88 posted by the Imgur user tarakan72511 and a person depicted in Odnoklassniki profiles

tarakan 72511

tarakan72511@chatme[.]im

paranoy7 77

daykalif@xmpp[.]jp
tarakan72511@chatme.im

daykalif

Tessa88

tarakan72511@chatme[.]im

DONAKOV MAKSIM

khaym@exploit[.]im
Bruno123123@yax[.]im
demigrooop@exploit[.]im

Khaim

ibmZZaODAY

Paranoy777 -> Khaim Link

Executive Summary

Paranoy777, also known as "Khaym" and "0db2016", is a member of several cybercriminal communities, including the top-tier Exploit forum, and has been primarily operating in the Russian-speaking underground. The actor's earliest involvement in illegal activities can be attributed to his registration on Exploit forum in November 2015.

Who Was the Real Hacker?

SELLER

HACKER

DONAKOV MAKSIM

Tessa88@bk.ru Link to Denisova

(4862) 751-318
info@oreluniver.ru

ОРЛОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ имени И.С. Тургенева 100 1919–2019

ВИДЫ ДЕЯТЕЛЬНОСТИ | ОБРАЗОВАТЕЛЬНАЯ | НАУЧНАЯ | МЕЖДУНАРОДНАЯ | СОЦИАЛЬНАЯ | ВОСПИТАТЕЛЬНАЯ | НАШ УНИВЕРСИТЕТ

Денисова Татьяна Геннадьевна

Занимаемые должности:
инженер Контрактная служба

Контактная информация

Образование:
В 2006 году окончила среднюю общеобразовательную школу № 20 им. Героя Советского Союза Л.Н. Гуртьева. В 2011 году, с отличием окончила ФГБОУ ВПО "Госуниверситет-УНПК " по специальности "Автоматизация технологических процессов и производств".

Квалификация:
инженер

Повышение квалификации и профессиональная переподготовка:
С 2011-2014 . проходила обучение в аспирантуре по специальности 05.13.06 "Автоматизация и управление технологическими процессами и производствами (по отраслям)."

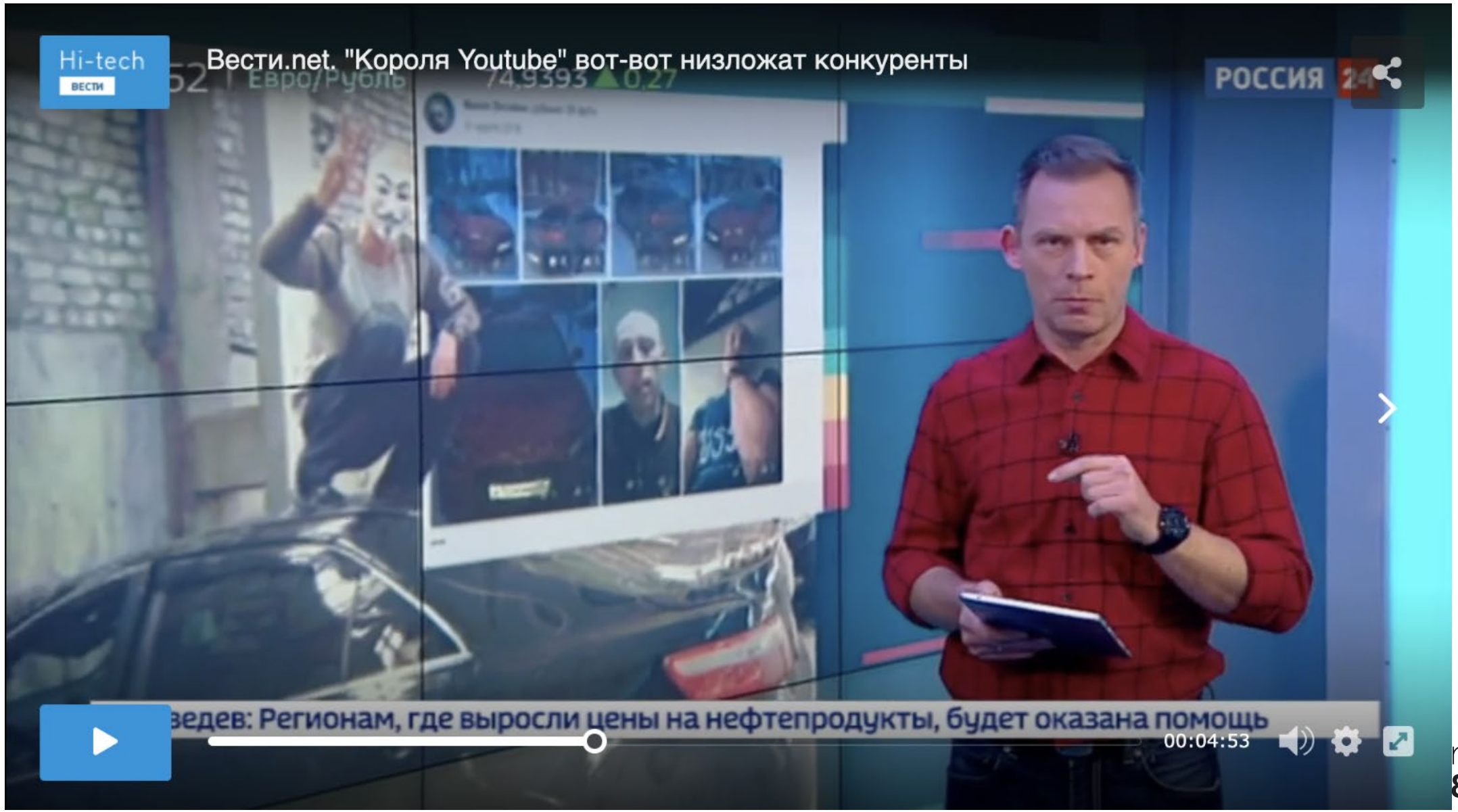
Общий стаж работы: 5

Стаж работы по специальности: 3

Преподаваемые дисциплины:

Дополнительная информация:

Rise to Fame


Hi-tech
ВЕСТИ
Вести.net. "Короля Youtube" вот-вот низложат конкуренты
РОССИЯ
ведев: Регионам, где выросли цены на нефтепродукты, будет оказана помощь
00:04:53

Other Known Indicators Used by paranoy777 aka tessa88

- Usernames:
  - 0db2016
  - khaym
- Jabbers:
  - paranoy777@exploit[.]im
  - khaym@exploit[.]im
  - Bruno123123@yax[.]im
  - demigrooop@exploit[.]im
  - tarakan72511@chatme[.]im
  - tanchik72511@exploit[.]im
  - db2016@swissjabber[.]ch
- Email addresses:
  - paraplan@mail[.]ru
- Skype:
  - Paranoy7771
- ICQ:
  - 709651701
- Web Money Wallets:
  - 947404114680
  - R125631224396
  - Z811745473923

New tessa88`s Indicators Were Revealed During Investigation

- Yahoo Massenger:
  - Tools.master2011
- M.Donakov`s Phone Numbers:
  - +79022222229
  - +17789981919
- Bitcoin Wallet:
  - 1HNXAXVQGw7RZ4sg2CjDMjpnhm36VHQSXJ

Key Take-Aways

- Evaluate Internal resources and identify the high-value/high-risk data.
- If budget permits, establish internal threat-intelligence program. At minimum provide additional training to the existing security personal
- Conduct threat-exposure research
  - Who
  - How
  - Why
- Maintain record of existing and emerging threats
  - Actors
  - Malware
  - TTP
- Prepare mitigation and contingency plan

RSAConference2019
Asia Pacific & Japan

Thank You

Andrei Barysevich

@DeepSpaceEye